

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2004 年 5 月 6 日 (06.05.2004)

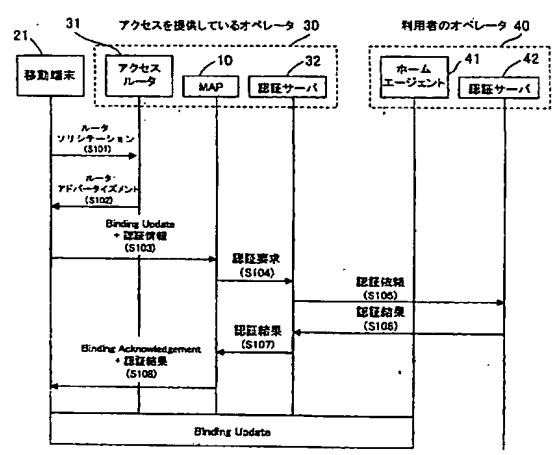
PCT

(10) 国際公開番号
WO 2004/039116 A1

- (51) 国際特許分類⁷: H04Q 7/38, H04L 12/56
- (21) 国際出願番号: PCT/JP2003/013624
- (22) 国際出願日: 2003 年 10 月 24 日 (24.10.2003)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2002-311910
2002 年 10 月 25 日 (25.10.2002) JP
- (71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府 門真市 大字門真 1 0 0 6 番地 Osaka (JP).
- (72) 発明者: 田中 武志 (TANAKA, Takeshi) [JP/JP]; 〒239-0847 神奈川県 横須賀市 光の丘 6-2-4 0 6 Kanagawa (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてののみ): 青山 高久 (AOYAMA, Takahisa) [JP/JP]; 〒233-0007 神奈川県 横浜市 港南区 大久保 3-4-1-3 1 6 Kanagawa (JP).
- (74) 代理人: 二瓶 正敬 (NIHEI, Masayuki); 〒160-0022 東京都 新宿区 新宿 2-8-8 とみん新宿ビル 2 F Tokyo (JP).
- (81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR,
- [続葉有]

(54) Title: RADIO COMMUNICATION MANAGEMENT METHOD AND RADIO COMMUNICATION MANAGEMENT SERVER

(54) 発明の名称: 無線通信管理方法及び無線通信管理サーバ



- 21...MOBILE TERMINAL
30...ACCESS PROVIDING OPERATOR
31...ACCESS ROUTER
32...AUTHENTICATION SERVER
40...USER OPERATOR
41...HOME AGENT
42...AUTHENTICATION SERVER
S101...ROUTER SOLICITATION
S102...ROUTER ADVERTISEMENT
S103...BINDING UPDATE AND AUTHENTICATION INFORMATION
S104...AUTHENTICATION REQUEST
S105...AUTHENTICATION ORDER
S106...AUTHENTICATION RESULT
S107...AUTHENTICATION RESULT
S108...BINDING ACKNOWLEDGEMENT AND AUTHENTICATION RESULT

(57) Abstract: The present invention allows a mobile terminal to smoothly perform a handover when changing link connections, and further shortens the time required for changing link connections. When a mobile terminal (21) changes connection links by use of HMIPv6, it transmits authentication information, at the same time as a transmission of information for changing the link connections (Binding Update), to a server (MAP10) that manages link connections of the mobile terminal. When the MAP requests an authentication server (32) for an authentication and acquires an authentication result, then it transmits the authentication result at the same as a transmission of affirmation information of the link connection change (Binding Acknowledgement). Alternatively, the MAP, after receiving the Binding Update and the authentication information from the mobile terminal, may firstly transmit the Binding Acknowledgement and a temporary permission of connection, and then acquire the authentication result to determine whether a formal permission of connection should be given.

(57) 要約: 移動端末がリンク接続を変更する際に、スムーズにハンドオーバーを行えるようにするとともに、リンク接続の変更に必要な時間を短縮することを目的とし、HMIPv6を利用して、移動端末21が接続リンクの変更を行う際、移動端末のリンク接続を管理するサーバ(MAP10)に対して、リンク接続を変更するための情報(Binding Update)と同時に、認証情報の送信を行う。MAPは、認証サーバ32に対して認証要求を行って認証結果を取得した場合、リンク接続の変更の承認情報(Binding Acknowledgement)と同時に、認証結果の送信を行う。また、MAPは、移動端末からBinding Updateと認証情報を受信した後、先に

Binding Acknowledgementと仮の接続許可を送り、その後、認証結果を取得して、正式な接続許可を与えるか否かを決定することも可能である。



HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

- 国際調査報告書
- 請求の範囲の補正の期限前の公開であり、補正書受領の際には再公開される。

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR),

2 文字コード及び他の略語については、定期発行される各 *PCT* ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明 細 書

無線通信管理方法及び無線通信管理サーバ

5 技術分野

本発明は、移動端末がリンク接続を変更する際に、通信が途切れないように移動端末のアドレスの変更を行う無線通信管理システム及び無線通信管理サーバに関し、特に、H M I P v 6 (Hierarchical Mobile IP version 6: 階層型モバイル I P v 6) を用いて移動端末のリンク接続を
10 管理する無線通信システムにおける無線通信管理方法及び無線通信管理サーバに関する。

背景技術

利用者が、移動端末 (Mobile Terminal) を利用してネットワークと通信を行う場合、アクセスを提供しているオペレータは、移動端末とネットワークとの接続サービスを提供する前に、移動端末がネットワークと接続する権利を有するか否かを判定 (認証) する必要がある。この認証処理は、アクセスを提供しているオペレータの施設である中間ノードが、移動端末に対してネットワークとの接続サービスを提供する前に、移動
20 端末からの接続要求に含まれる認証情報 (端末 I D 及び利用者情報の組合せ) を認証サーバに問い合わせ、認証サーバからの応答に含まれる認証結果に従って、移動端末に対するネットワークとの接続サービスを提供するか否かを判断することにより実現される。なお、必要に応じて、ネットワークを介して、利用者のオペレータの施設に存在する所定の認証サーバに対して認証を依頼することも可能である。本明細書では、このシーケンスを認証シーケンスと呼ぶことにする。

25

例えば、後述の非特許文献 1 に記載の技術である IEEE802.11x を無線 LAN に適用した場合には、移動端末が、ネットワークと接続する際の入り口となるアクセスポイント (Access Point) と接続する際にアクセスポイントに認証情報を送り、アクセスポイントが移動端末の認証サーバ
5 に対して認証要求を行うことによって認証処理の実現が可能となっている。

ところで近年、移動端末のワイヤレス化に伴い、移動端末が利用する中間ノードを連続的に切り替えて移動しながら、ネットワークとの継続的な通信を行う場合が増えている。この場合、移動端末にパケットを届
10 けるためには、ネットワーク内のいずれかのノードが、何らかの方法で移動端末の位置を特定する機能を有する必要がある。この移動端末の位置を特定する機能を有するノードは、位置管理サーバと呼ばれ、通常、移動端末の所属する利用者のオペレータに設置される (すなわち、移動端末は、利用者のオペレータの加入者である)。

15 移動端末がネットワークとの通信を継続しながら、利用する中間ノードを切り替えるシームレスハンドオーバーは、通常、ネットワーク内に設置された位置管理サーバに対して、移動端末が位置登録を行うことにより実現可能である。なお、本明細書では、このシーケンスを位置登録シーケンスと呼ぶことにする。

20 なお、認証シーケンスと位置登録シーケンスとは、シーケンスに係るノードが異なっている。すなわち、認証シーケンスでは、移動端末とネットワークへのアクセスを提供しているドメイン内のサーバとの通信が行われるのに対し、位置登録シーケンスでは、移動端末とネットワーク内の位置管理サーバとの通信が行われる。

25 移動端末は、認証シーケンスや位置登録シーケンスが完了するまでの間、ネットワークとの通信を行うことができないため、これらのシーケ

ンスはできるだけ短いことが望ましい。このため、後述の非特許文献 2 に記載されているように、認証シーケンスと位置登録シーケンスとを組み合わせる Diameter Mobile IPv4 Application が考えられている。この Diameter Mobile IPv4 Application は、IPv4 環境下でシームレスハンド
5 オーバを可能とする技術である後述の非特許文献 3 記載の Mobile IPv4 シーケンス中に、上記のシーケンスを含めるものである。

図 9 は、従来の技術に係る Diameter Mobile IPv4 Application のシーケンスを示す図である。図 9 には、利用者がネットワーク 5 4 と接続して通信を行うために利用する移動端末 5 1、移動端末 5 1 に対してネットワーク 5 4 へのアクセスを提供しているオペレータ 5 7 内のフォーリン
10 エージェント 5 2 及び認証サーバ 5 3、ネットワーク 5 4、ネットワーク 5 4 上に存在し、利用者の端末のアドレスを管理する利用者のオペレータ 5 8 内に配置されたホームエージェント 5 5 及び認証サーバ 5 6 が図示されている。

15 Mobile IPv4 機能を搭載した移動端末は、アクセスを提供しているオペレータ 5 7 内（フォーリンネットワーク）に設置された中間ノード（フォーリンエージェント 5 2）経由で、位置管理サーバ（ホームエージェント 5 5）に対して位置登録シーケンスを行う。Diameter Mobile IPv4 Application では、Mobile Node が位置登録を行う際に、フォーリンエ
20 ジェント 5 2 に対して送信する位置登録メッセージ（Binding Update）内に、移動端末 5 1 の認証情報が付加され、フォーリンエージェント 5 2 が、アクセスを提供しているオペレータ 5 7 内の認証サーバ 5 3 又は利用者のオペレータ 5 8 内の認証サーバ 5 6 に対して認証要求を行うことにより、認証シーケンスが可能となっている。

25 一方、移動端末が、ネットワーク上の接続リンクを変更した場合でも、ある特定のアドレス（IP アドレス）を用いて通信することを可能とし、

現在継続中の通信を中断することなくシームレスに接続リンクの変更を可能とするMobileIPv6技術の標準化がIETFのMobile IP Working Groupにおいて進められている。このIPv6環境におけるシームレスハンドオーバをサポートするプロトコルであるMobile IPv6（後述の非特許文献4参照）の位置登録シーケンスは、Mobile IPv4で規定されていたフォーリンエージェント52のような『アクセスを提供しているオペレータ57内の中間ノード』を経由せずに行われる。

Mobile IPv6では、基本的に下記の1～3の動作によって、移動端末がアクセスリンク（アクセスネットワーク）に接続中も、ホームアドレス宛てのパケットを受け取ることが可能となる。

1. Care-of Addressの取得

Mobile Nodeは、接続するリンクをアクセスリンクに変更すると、まずそのアクセスリンクより、そのリンク上のIPアドレス(CoA:Care-of Address)を取得する。これは通常、アクセスルータから定期的にアクセスリンク上の全端末に向けて広告されるルータアドバータイズメント(Router Advertisement)を受信するか、DHCPv6を用いることで実現される。

2. Binding UpdateとBinding Acknowledgement

次に、移動端末は、自分のホームエージェントに対して、その移動端末のホームアドレスとCoAとの組を報告する(Binding Update)。報告を受けたホームエージェントは、その組をテーブルとして保存する。移動端末は接続するリンクを変更する度に、このBinding Updateを行う。ホームエージェントはBinding Updateに対してBinding Acknowledgementを返すが、この過程はBinding Updateにその指示があったときのみ行う。

25 3. IPトンネリング

この後、ホームエージェントは、移動端末と通信中の端末（

- Correspondent Node) からホームリンク (ホームネットワーク) に届いたパケットのうちのテーブル内に登録されたホームアドレス宛てのパケットを、テーブル内に登録された C o A 宛ての I P パケット内のペイロード部分に挿入し、登録されている C o A 宛ての I P ヘッダを付加して、
- 5 I P ネットワークに転送する (I P トンネリング)。転送されたパケットは I P ヘッダの C o A に従ってアクセスリンク上に届き、そこから移動端末に配送される。移動端末は、そのパケットのペイロード部分を取得することにより、アクセスリンクに接続しながら、ホームアドレス宛てのパケットを受け取ることができる。
- 10 しかしながら、IPv6では、移動端末が接続するリンクを変更した場合、Binding Updateが完了するまでの間は、以前接続していたリンク (接続変更前に接続していたリンク) に、自分のホームアドレス宛てのパケットが届いてしまうことになり、この間は新しい接続リンク先で自分のホームアドレス宛てのパケットを受け取ることが不可能となる。特に、移
- 15 動端末からホームエージェントまでのネットワーク上の距離 (中継するルータ数、中継データリンクの容量などに依存する距離) が離れている場合には、移動端末がホームエージェントにBinding Updateを行うのに必要な時間が長くなり、移動端末が自分のホームアドレス宛てのパケットを受け取れない時間が長くなってしまうという問題点がある。
- 20 この問題に対する 1 つのアプローチとして、後述の非特許文献 5 に記載されているように、アクセスリンクから比較的近いリンクで構成されたネットワーク上に、新たに移動端末の位置管理を行うサーバを設置し、移動端末がそのネットワーク内でアクセスリンクを変更した場合には、そのサーバに対してCare-of Addressを登録することにより、Binding
- 25 Update完了までに要する時間を短縮する階層型MobileIPv6 (Hierarchical MIPv6 : HMIPv6) が、Mobile IP Working Groupで提案され

、現在標準化が行われている。なお、このHMIPv6は、MobileIPv6と共存して動作可能である。

図10は、従来の技術に係るHMIPv6のシーケンスを示す図である。

HMIPv6では、アクセスを提供しているオペレータ64にMAP (Mobility Anchor Point) と呼ばれる移動端末61の比較的狭いリンク内の移動を管理するサーバを設けている。なお、MAPが管理するリンクはMAPドメインと呼ばれ、MAP62は通常、MAPドメイン内の上位ネットワークに近い側に設置される。HMIPv6では、次のような動作によって、移動端末61がMAPドメイン内で移動する場合のBinding過程に必要な時間を短縮することを可能とする。

移動端末61が、新たにMAPドメインに入るか、又は、異なるMAPドメインに移動して接続リンクを変更した場合、まずアクセスリンクより、そのリンク上のLCoA (通常のCoA: On-Link CoA) を取得し、さらに移動端末61は、このアクセスリンク上のMAP62のアドレスを取得する。移動端末61は、そのMAP62のアドレスから、移動端末61の別のCoA (RCOA: Regional CoA) を構成する。そして、移動端末61は、自端末のRCOAとLCoAとの組を、そのMAP62に対して登録する (内部位置登録)。MAP62はこの登録に対して、OKの場合には、Binding Acknowledgementを返すとともに、移動端末61に対して、外部への接続サービスを提供する。また、さらに移動端末61は、利用者のオペレータ65のホームエージェント (自端末のホームエージェント) 63に対してRCOAの登録を行う。 (位置登録シーケンス)。

このような位置登録をしておくことによって、移動端末61が同じMAPドメイン内の異なるリンクに接続を変更した場合には、移動端末61は、MAP62に対してLCoAの登録のみを行えばよく、ホームエ

エージェント 63 への L C o A の登録は不要となる。したがって、移動端末 61 が M A P ドメイン内を移動する場合であれば、ホームエージェント 63 に C o A を登録 (Binding Update) し、その確認 (Binding Acknowledgement) を受信する一連の Binding 過程は省略され、ホームアドレス宛てのパケットを受信できない時間が短縮される。

すなわち、HMIPv6 では、移動端末 61 が新たに M A P ドメイン内のリンクに接続するか、M A P ドメインを変更する場合には、移動端末 61 は、M A P 62 への R C o A と L C o A との組の登録、及び、ホームエージェント 63 への R C o A の登録が必要となるが、移動端末 61 が M A P ドメイン内で接続リンクを変更する場合には、M A P 62 への L C o A の登録のみを行えばよく、M A P ドメイン内での移動時の Binding 過程に要する時間を短縮するのに有効である。

非特許文献 1

IEEE 802.1 Working Group, "Port-Based Network Access Control", IEEE 802.1x Standard, June 2001.

非特許文献 2

Pat R. Calhoun, Tony Johansson, etc., "Diameter Mobile IPv4 Application", Internet Draft, draft-ietf-aaa-diameter-mobileip-13, Oct 2002, Work In Progress.

20 非特許文献 3

Perkins. C, "Mobility Support for IPv4", RFC3220, Jan 2002

非特許文献 4

C. Perkins, Jari A., etc., "Mobility Support in IPv6", Internet Draft, draft-ietf-mobileip-ipv6-18, Jun 2002, Work In Progress.

25 非特許文献 5

H. Soliman, C. Castelluccia, etc., "Hierarchical Mobile IPv6

mobility management (HMIPv6)" Internet Draft,
draft-ietf-mobileip-hmipv6-07, Oct 2002, Work In Progress.

- MobileIPv6及びHMIPv6を実際に用いる場合、アクセスを提供しているオペレータと利用者のオペレータとは異なる場合が多く、リンク接続を試みる移動端末に対して認証を行う必要性がある。このためには、移動
- 5 端末に対して、IP網の所定のネットワークとの接続サービスを提供する前に、サービスを提供するオペレータが、移動端末から認証情報を取得し、その認証情報を用いて認証処理を行い、認証結果に応じて、接続サービスを提供するか否かを決定する必要がある。
- 10 現在、これらの処理を行う条件を満たすものとしては、IEEE802.1xなどのIPレベルでの接続を確立するより前に認証を行う技術が挙げられるが、端末の認証の間や、Binding過程（Binding Update及びBinding Acknowledgementのやり取り）が完了するまでの間、移動端末にはIP網からのパケットが届かないことになってしまい、シームレスハンドオー
- 15 バを実現することは困難となっている。

発明の開示

- 上記課題に鑑み、本発明は、移動端末がリンク接続を変更するハンドオーバー時に、スムーズにハンドオーバーを行えるようにするとともに、リンク接続の変更に必要な時間を短縮することを可能とする無線通信管理
- 20 システム及び無線通信管理サーバを提供することを目的とする。

- 上記目的を達成するため、本発明では、HMIPv6を用いて移動端末のリンク接続を管理する無線通信システムにおける無線通信管理方法に関し、移動端末のリンク接続を管理するサーバに対して、移動端末が、
- 25 リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を送信し、移動端末のリンク接続の変更

に要する時間を短縮するようにしている。

これにより、HMI P v 6において、移動端末がリンク接続を変更するハンドオーバー時に、認証シーケンスと位置登録シーケンスとを同時に実行し、リンク接続の変更に必要な時間を短縮することが可能となる。

- 5 さらに、本発明では、上記発明に加えて、移動端末が、リンク接続を変更するための情報と、認証に係る情報とを1つの情報として送信し、リンク接続を管理するサーバが、1つの情報から、リンク接続を変更するための情報及び認証に係る情報のそれぞれを取得するようにしている。

- 10 これにより、移動端末は、1つの情報の送信を行うだけで、認証要求及び位置登録要求を行うことが可能となる。

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、認証に係る情報を用いた認証処理による認証結果を取得するようにしている。

- 15 これにより、認証要求及び位置登録要求を受けたサーバが、認証結果の取得を行うことが可能となる。

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、移動端末の認証を行う認証サーバとの通信を行い、認証結果を取得するようにしている。

- 20 これにより、認証要求及び位置登録要求を受けたサーバが、認証サーバに認証依頼を送信し、認証サーバでの認証結果を受信することが可能となる。

さらに、本発明では、上記発明に加えて、移動端末のリンク接続の変更を確認した旨を通知する情報と、認証結果とを1つの情報として、移動端末に送信するようにしている。

- 25 これにより、1つの情報の送信によって、認証要求及び位置登録要求を受けたサーバが、移動端末に対してリンク接続の変更の確認情報と認

証結果とを送信できるようになるとともに、認証結果の送信タイミングを定めることが可能となる。

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、移動端末のリンク接続の変更を確認した旨を通知する情報を移動
5 端末に送信し、その後、認証結果を取得できた場合に認証結果を移動端末に送信するようにしている。

これにより、認証要求及び位置登録要求を受けたサーバは、時間がかかると予想される認証結果の取得を待つことなく、まず、リンク接続の変更の確認情報を移動端末に返すことが可能となる。

10 さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、認証結果の取得までの時間を設定し、認証結果の取得までの時間内に認証結果を取得できた場合、次に移動端末からリンク接続を変更するための情報を受信した際に、移動端末のリンク接続の変更を確認した旨を通知する情報と共に、認証結果を移動端末に送信するようにしてい
15 る。

これにより、認証要求及び位置登録要求を受けたサーバが認証結果を取得した場合に、移動端末に対して認証結果を送信するタイミングを定めることが可能となる。

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、移動端末が所望のネットワークへのアクセスを仮許可する所定の
20 仮許可時間を設定し、移動端末のリンク接続の変更を確認した旨を通知する情報と共に、所定の時間だけ所望のネットワークへのアクセスの許可を通知する情報を移動端末に送信するようにしている。

これにより、認証処理が終わっていない移動端末に対しても接続許可
25 が与えられ、認証処理が完了するのを待つことなく移動端末は、通信を継続することが可能となる。

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、所定の仮許可時間よりも長い時間であって、移動端末が所望のネットワークへのアクセスを許可する所定の許可時間を設定し、認証結果が認証成功であった場合、移動端末のリンク接続の変更を確認した旨を
5 通知する情報と共に、所定の許可時間だけ所望のネットワークへのアクセスの許可を通知する情報を移動端末に送信するようにしている。

これにより、認証に成功した移動端末に対しては、十分に長い有効時間が設定された接続許可を与えることが可能となる。

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、所定の仮許可時間又は所定の許可時間だけ所望のネットワークへの
10 アクセスを許可した移動端末のリンク接続の変更に係る登録を行い、所定の仮許可時間又は所定の許可時間が経過した場合、移動端末のリンク接続の変更に係る登録を削除するようにしている。

これにより、認証が行われている時間だけ移動端末に与えられていた
15 接続許可や、十分に長い時間だけ移動端末に与えられていた接続許可の有効時間が切れた場合、移動端末をリンクから離すことによって、不正なリンク接続が起こらないようにすることが可能となる。

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、認証結果の取得までの時間を設定し、認証結果の取得までの時間
20 内に認証結果を取得できなかった場合、認証結果を認証失敗とするようにしている。

これにより、例えば、認証サーバとの通信が不可能となり、移動端末に係る認証結果が取得できない場合に、移動端末に対して、接続許可を与えないようにすることが可能となる。

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、移動端末に対して所定の接続禁止時間を設定し、移動端末に対し
25

て認証結果として認証失敗を通知した場合には、認証失敗の通知から所定の接続禁止時間だけ、認証失敗であった移動端末のリンク接続の変更に係る処理及び認証に係る処理を行わないようにしている。

これにより、認証に失敗した移動端末に対して、所定の時間だけ接続
5 禁止の設定を行い、リンク接続の変更要求や認証要求を受けないようにすることで、特に、繰り返し行われる不正なアクセスを防止することが可能となる。

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、移動端末に対して認証結果として認証成功を通知した場合のみ、
10 認証成功であった移動端末のリンク接続の変更に係る登録を行うようにしている。

これにより、認証に成功した移動端末のアドレスのみを登録することが可能となる。

また、上記目的を達成するため、本発明では、移動端末のリンク接続
15 を管理する無線通信システムにおける無線通信管理方法に関し、移動端末のリンク接続を管理するサーバに対して、移動端末が、リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を送信し、リンク接続を管理するサーバが、認証に係る情報を用いた認証処理による認証結果の取得までの時間を設定し、認
20 証結果の取得までの時間内に認証結果を取得できた場合、認証結果を前記移動端末に送信するようにしている。

これにより、認証要求を受けたサーバが認証結果を取得した場合に、移動端末に対して認証結果を送信するタイミングを定めることが可能となる。

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、移動端末が所望のネットワークへのアクセスを仮許可する所定の

25

仮許可時間を設定し、所定の時間だけ所望のネットワークへのアクセスの許可を通知する情報を移動端末に送信するようにしている。

これにより、認証処理が終わっていない移動端末に対しても接続許可が与えられ、認証処理が完了するのを待つことなく移動端末は、通信を
5 継続することが可能となる。

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、所定の仮許可時間よりも長い時間であって、移動端末が所望のネットワークへのアクセスを許可する所定の許可時間を設定し、認証結果が認証成功であった場合、所定の許可時間だけ所望のネットワークへの
10 アクセスの許可を通知する情報を移動端末に送信するようにしている。

これにより、認証に成功した移動端末に対しては、十分に長い有効時間が設定された接続許可を与えることが可能となる。

さらに、本発明では、上記発明に加えて、所定の仮許可時間又は所定の許可時間が経過した場合、リンク接続を管理するサーバは、移動端末
15 の接続を切断するようにしている。

これにより、認証が行われている時間だけ移動端末に与えられていた接続許可や、十分に長い時間だけ移動端末に与えられていた接続許可の有効時間が切れた場合、移動端末をリンクから離す（ネットワークから切断する）ことによって、不正なリンク接続が起こらないようにするこ
20 とが可能となる。

また、上記目的を達成するため、本発明では、上記発明に加えて、移動端末のリンク接続を管理する無線通信システムにおける無線通信管理方法に関し、移動端末のリンク接続を管理するサーバに対して、移動端末が、リンク接続を変更するための情報と同時に、所望のネットワーク
25 にアクセスするための認証に係る情報を送信し、リンク接続を管理するサーバが、認証に係る情報を用いた認証処理による認証結果の取得まで

の時間を設定し、認証結果の取得までの時間内に認証結果を取得できなかった場合、認証結果を認証失敗とするようにしている。

これにより、例えば、認証サーバとの通信が不可能となり、移動端末に係る認証結果が取得できない場合に、移動端末に対して、接続許可を
5 与えないようにすることが可能となる。

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、移動端末に対して所定の接続禁止時間を設定し、移動端末に対して認証結果として認証失敗を通知した場合には、認証失敗の通知から所定の接続禁止時間だけ、認証失敗であった移動端末に係る処理を行わな
10 いようにしている。

これにより、認証に失敗した移動端末に対して、所定の時間だけ接続禁止の設定を行い、リンク接続の変更要求や認証要求を受けないようにすることで、特に、繰り返し行われる不正なアクセスを防止することが可能となる。

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、移動端末に対して認証結果として認証成功を通知した場合のみ、認証成功であった移動端末のリンク接続の変更に係る登録を行うようにしている。

これにより、認証に成功した移動端末のアドレスのみに接続許可を与えることが可能となる。
20

また、上記目的を達成するため、本発明では、HMI P v 6 を用いて移動端末のリンク接続を管理する無線通信管理サーバに関し、移動端末から、リンク接続を変更するための情報と所望のネットワークにアクセスするための認証に係る情報とを1つの情報で受信し、1つの情報から、
25 リンク接続を変更するための情報及び認証に係る情報のそれぞれを取得するよう構成している。

この構成により、移動端末は、1つの情報の送信を行うだけで、認証要求及び位置登録要求を行うことが可能となる。

さらに、本発明では、上記発明に加えて、認証に係る情報を用いた認証処理による認証結果を取得するよう構成している。

- 5 この構成により、認証要求及び位置登録要求を受けたサーバが、認証結果の取得を行うことが可能となる。

さらに、本発明では、上記発明に加えて、移動端末の認証を行う認証サーバとの通信を行う手段を有し、認証結果を取得するよう構成している。

- 10 この構成により、認証要求及び位置登録要求を受けたサーバが、認証サーバに認証依頼を送信し、認証サーバでの認証結果を受信することが可能となる。

さらに、本発明では、上記発明に加えて、移動端末のリンク接続の変更を確認した旨を通知する情報と認証結果とを1つの情報として、移動

- 15 端末に送信するよう構成している。

この構成により、1つの情報の送信によって、認証要求及び位置登録要求を受けたサーバが、移動端末に対してリンク接続の変更の確認情報と認証結果とを送信できるようになるとともに、認証結果の送信タイミングを定めることが可能となる。

- 20 さらに、本発明では、上記発明に加えて、移動端末のリンク接続の変更を確認した旨を通知する情報を移動端末に送信し、その後、認証結果を取得できた場合に認証結果を移動端末に送信するよう構成している。

この構成により、認証要求及び位置登録要求を受けたサーバは、時間がかかると予想される認証結果の取得を待つことなく、まず、リンク接

- 25 続の変更の確認情報を移動端末に返すことが可能となる。

さらに、本発明では、上記発明に加えて、認証結果の取得までの時間

を設定する時間設定手段を有し、認証結果の取得までの時間内に認証結果を取得できた場合、次に移動端末からリンク接続を変更するための情報を受信した際に、移動端末のリンク接続の変更を確認した旨を通知する情報と共に、認証結果を移動端末に送信するよう構成している。

- 5 この構成により、認証要求及び位置登録要求を受けたサーバが認証結果を取得した場合に、移動端末に対して認証結果を送信するタイミングを定めることが可能となる。

- さらに、本発明では、上記発明に加えて、移動端末に対して所望のネットワークへのアクセスを仮許可する所定の仮許可時間を設定する時間
10 設定手段を有し、移動端末のリンク接続の変更を確認した旨を通知する情報と共に、所定の時間だけ所望のネットワークへのアクセスの許可を通知する情報を移動端末に送信するよう構成している

- この構成により、認証処理が終わっていない移動端末に対しても接続許可が与えられ、認証処理が完了するのを待つことなく移動端末は、通
15 信を継続することが可能となる。

- さらに、本発明では、上記発明に加えて、移動端末に対して、所定の仮許可時間よりも長い時間であって、移動端末が所望のネットワークへのアクセスを許可する所定の許可時間を設定する時間設定手段を有し、認証結果が認証成功であった場合、移動端末のリンク接続の変更を確認
20 した旨を通知する情報と共に、所定の許可時間だけ所望のネットワークへのアクセスの許可を通知する情報を移動端末に送信するよう構成している。

この構成により、認証に成功した移動端末に対しては、十分に長い有効時間が設定された接続許可を与えることが可能となる。

- 25 さらに、本発明では、上記発明に加えて、所定の仮許可時間又は所定の許可時間だけ所望のネットワークへのアクセスを許可した移動端末の

リンク接続の変更に係る登録を行う情報登録手段と、所定の仮許可時間又は所定の許可時間が経過した場合、移動端末のリンク接続の変更に係る登録を削除する情報削除手段とを有するよう構成している。

- この構成により、認証が行われている時間だけ移動端末に与えられていた接続許可や、十分に長い時間だけ移動端末に与えられていた接続許可の有効時間が切れた場合、移動端末をリンクから離すことによって、不正なリンク接続が起こらないようにすることが可能となる。

- さらに、本発明では、上記発明に加えて、認証結果の取得までの時間を設定する時間設定手段と、認証結果の取得までの時間内に認証結果を取得できなかった場合、認証結果を認証失敗とする判定手段とを有するよう構成している。

この構成により、例えば、認証サーバとの通信が不可能となり、移動端末に係る認証結果が取得できない場合に、移動端末に対して、接続許可を与えないようにすることが可能となる。

- さらに、本発明では、上記発明に加えて、移動端末に対して所定の接続禁止時間を設定する時間設定手段と、移動端末に対して認証結果として認証失敗を通知した場合には、認証失敗の通知から所定の接続禁止時間だけ、認証失敗であった移動端末のリンク接続の変更に係る処理及び認証に係る処理を行わないよう制御する制御手段とを有するよう構成している。

この構成により、認証に失敗した移動端末に対して、所定の時間だけ接続禁止の設定を行い、リンク接続の変更要求や認証要求を受けないようにすることで、特に、繰り返し行われる不正なアクセスを防止することが可能となる。

- さらに、本発明では、上記発明に加えて、移動端末に対して認証結果として認証成功を通知した場合のみ、認証成功であった移動端末のリン

ク接続の変更に係る登録を行うよう制御する制御手段を有するよう構成している。

この構成により、認証に成功した移動端末のアドレスのみを登録することが可能となる。

- 5 また、上記目的を達成するため、本発明では、移動端末のリンク接続を管理する無線通信管理サーバに関し、移動端末から、リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を受信する受信手段と、認証に係る情報を用いた認証処理による認証結果の取得までの時間を設定する時間設定手段と、認証結果の取得までの時間内に認証結果を取得できた場合、認証結果を移動端末に送信する送信手段とを有している。

この構成により、認証要求を受けたサーバが認証結果を取得した場合に、移動端末に対して認証結果を送信するタイミングを定めることが可能となる。

- 15 さらに、本発明では、上記発明に加えて、移動端末が所望のネットワークへのアクセスを仮許可する所定の仮許可時間を設定する時間設定手段を有し、所定の時間だけ所望のネットワークへのアクセスの許可を通知する情報を移動端末に送信するよう構成している。

- 20 この構成により、認証処理が終わっていない移動端末に対しても接続許可が与えられ、認証処理が完了するのを待つことなく移動端末は、通信を継続することが可能となる。

- 25 さらに、本発明では、上記発明に加えて、所定の仮許可時間よりも長い時間であって、移動端末が所望のネットワークへのアクセスを許可する所定の許可時間を設定する時間設定手段を有し、認証結果が認証成功であった場合、所定の許可時間だけ所望のネットワークへのアクセスの許可を通知する情報を移動端末に送信するよう構成している。

この構成により、認証に成功した移動端末に対しては、十分に長い有効時間が設定された接続許可を与えることが可能となる。

さらに、本発明では、上記発明に加えて、所定の仮許可時間又は所定の許可時間が経過した場合、移動端末の接続を切断する制御手段を有している。

この構成により、認証が行われている時間だけ移動端末に与えられていた接続許可や、十分に長い時間だけ移動端末に与えられていた接続許可の有効時間が切れた場合、移動端末をリンクから離す（ネットワークから切断する）ことによって、不正なリンク接続が起こらないようにすることが可能となる。

また、上記目的を達成するため、本発明では、移動端末のリンク接続を管理する無線通信システムにおける無線通信管理サーバに関し、移動端末から、リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を受信する受信手段と、リンク接続を管理するサーバが、認証に係る情報を用いた認証処理による認証結果の取得までの時間を設定する時間設定手段と、認証結果の取得までの時間内に認証結果を取得できなかった場合、認証結果を認証失敗として、認証結果を移動端末に送信する送信手段とを有している。

この構成により、例えば、認証サーバとの通信が不可能となり、移動端末に係る認証結果が取得できない場合に、移動端末に対して、接続許可を与えないようにすることが可能となる。

さらに、本発明では、上記発明に加えて、移動端末に対して所定の接続禁止時間を設定する時間設定手段と、移動端末に対して認証結果として認証失敗を通知した場合には、認証失敗の通知から所定の接続禁止時間だけ、認証失敗であった移動端末に係る処理を行わないよう制御する制御手段とを有している。

この構成により、認証に失敗した移動端末に対して、所定の時間だけ接続禁止の設定を行い、リンク接続の変更要求や認証要求を受けないようにすることで、特に、繰り返し行われる不正なアクセスを防止することが可能となる。

- 5 さらに、本発明では、上記発明に加えて、移動端末に対して認証結果として認証成功を通知した場合のみ、認証成功であった移動端末のリンク接続の変更に係る登録を行うよう制御する制御手段を有している。

この構成により、認証に成功した移動端末のみを接続許可を与えることが可能となる。

10

図面の簡単な説明

図 1 は、本発明の第 1 の実施の形態における M A P の構成を示すブロック図、

図 2 は、本発明の第 1 の実施の形態におけるシーケンスを示す図、

- 15 図 3 は、本発明の第 2 の実施の形態における M A P の構成を示すブロック図、

図 4 は、本発明の第 2 の実施の形態におけるシーケンスを示す図、

図 5 は、本発明の第 2 の実施の形態における移動端末から Binding Update を受けた際の M A P の処理の詳細を示すフローチャート、

- 20 図 6 は、本発明の第 2 の実施の形態における状態テーブルの一例を示す模式図、

図 7 は、本発明の第 2 の実施の形態における認証サーバ 3 2 から認証結果を受信した場合及び所定の時間が経過した場合の M A P の処理の詳細を示すフローチャート、

- 25 図 8 は、本発明に係る状態テーブルの別の一例を示す模式図、

図 9 は、従来の技術に係る Diameter Mobile IPv4 Application のシー

ケンスを示す図、

図 10 は、従来の技術に係る HMIPv6 のシーケンスを示す図である。

発明を実施するための最良の形態

5 以下、図面を参照しながら、本発明の実施の形態について説明する。

(第 1 の実施の形態)

まず、図面を参照しながら、本発明の第 1 の実施の形態について説明
する。本発明の第 1 の実施の形態では、HMIPv6 (Hierarchical
Mobile IP version 6) の位置登録シーケンス中に認証シーケンスを含め
10 ることによって、ハンドオーバに要する時間を短縮し、シームレスな接
続サービスを提供することを可能とする技術について説明する。

図 1 は、本発明の第 1 の実施の形態における MAP の構成を示すブロッ
ク図である。図 1 に示す MAP (Mobility Anchor Point) 10 は、上位
ネットワーク 20 と接続する上位ネットワーク通信手段 11、下位ネ
15 ットワーク 25 と接続する下位ネットワーク通信手段 12、HMIPv6
を利用したデータ伝送の経路を決定及び制御する HMIPv6 経路制
御手段 13、認証サーバ 32 に対して認証要求の送信及び認証結果の受
信を行う認証要求送受信手段 14、データ伝送経路の設定の際に参照さ
れる HMIPv6 テーブル 16 と認証サーバ 32 のアドレス 17 とを格
20 納する情報格納手段 15 を有している。このうち、本発明の第 1 の実施
の形態に特徴的な構成要素は認証要求送受信手段 14 と、情報格納手段
15 に格納された認証サーバ 32 のアドレス 17 であり、上位ネットワ
ーク通信手段 11、下位ネットワーク通信手段 12、HMIPv6 経路
制御手段 13 は、従来から存在するものを利用することが可能である。
25 なお、MAP 10 はコンピュータによって実現可能であり、上記の各手
段は CPU などの中央処理手段によって実現可能であるとともに、様々

な情報の参照し、判断・判定処理を行うことも可能である。

図2は、本発明の第1の実施の形態におけるシーケンスを示す図である。図2には、利用者がネットワークと接続して通信を行うために利用する移動端末21、移動端末21によるネットワークへのアクセスを提供しているオペレータ30、利用者のオペレータ40が図示されている。また、アクセスを提供しているオペレータ30には、アクセスルータ31、MAP10、認証サーバ32が存在し、利用者のオペレータ40には、ホームエージェント41、認証サーバ42が存在する。なお、図2におけるMAP10は、図1に示す本発明を実施するためのMAP10である。

まず、移動端末21が新たなリンクに接続した場合、移動端末21はアクセスルータ31に対して、ルータアドバータイズメント (Router Advertisement) の送信を促すルータソリシテーション (Router Solicitation) を送信する (ステップS101)。このルータソリシテーションを受けて、アクセスルータ31は移動端末21に対して、IPアドレスなどのルータ情報を含むルータアドバータイズメントを送信する (ステップS102)。なお、アクセスルータ31がルータソリシテーションを受けずに、マルチキャストで定期的にルータアドバータイズメントを流すことも可能である。

移動端末21は、アクセスルータ31からのルータアドバータイズメントを受けて、接続したリンク上のIPアドレス (LCoA: On-link Care-of Address) を取得する。また、移動端末21の接続したリンクがMAP10ドメイン内のリンクである場合、このリンクでのMAP10の利用が可能であることがルータアドバータイズメントに示されており、HMIPv6を搭載した移動端末21は、MAP10のアドレスを取得することが可能である。そして、このMAP10のアドレスから、もう

1つのC o AであるR C o A (Regional Care-of Address) を構成する。

次に、H M I P v 6 を実装する移動端末 2 1 は、M A P 1 0 への Binding Update (バインディングアップデート：なお、B U と省略することもある) を行うための情報 (L C o A) と、端末 I D 及び利用者情報を含む認証情報とを、M A P 1 0 に対して送信する (ステップ S 1 0 3)。M A P 1 0 は、情報格納手段 1 5 内に格納されている認証サーバ 3 2 のアドレス 1 7 を参照し、認証要求送受信手段 1 4 を用いて、認証サーバ 3 2 に対して認証要求を送信する (ステップ S 1 0 4)。また、必要ならば、アクセスを提供しているオペレータ 3 0 の認証サーバ 3 2 は、利用者のオペレータ 4 0 の認証サーバ 4 2 に対して認証依頼を送信し (ステップ S 1 0 5)、認証処理後の応答 (認証結果) を受信する (ステップ S 1 0 6)。そして、認証サーバ 3 2 は M A P 1 0 に対して、認証結果を返す (ステップ S 1 0 7)。

なお、上記のステップ S 1 0 6 及びステップ S 1 0 7 の処理が必要でない場合 (アクセスを提供しているオペレータ 3 0 の認証サーバ 3 2 において、認証処理が可能な場合) には、アクセスを提供しているオペレータ 3 0 の認証サーバ 3 2 で認証処理を行って、その認証結果を M A P 1 0 に返すようにする。また、M A P 1 0 が、利用者のオペレータ 4 0 の認証サーバ 4 2 と認証依頼及び認証結果のやり取りを直接行うことも可能である。

一方、M A P 1 0 は、認証サーバ 3 2 への認証要求の送信と同時に R C o A 及び L C o A の登録 (Binding Update) を行う。M A P 1 0 は、R C o A 及び L C o A の登録が完了し、かつ、認証サーバ 3 2 から認証結果を受けた時点で、Binding Acknowledgement (バインディングアクノ
レッジメント：なお、B A と省略することもある) と認証結果とを移動
端末 2 1 に対して送信する (ステップ S 1 0 8)。

上記までの動作が終了すると、その後は従来と同様のHMI P v 6におけるホームエージェント41へのBinding Updateが行われる。すなわち、移動端末21は、RC o Aをホームエージェント41に送信して、ホームエージェント41から登録されたことを示すBinding

5 Acknowledgementを受信する。

以上、説明したように、本発明の第1の実施の形態によれば、シームレスハンドオーバを目的とし、すでに標準化が進められているHMI P v 6の位置登録シーケンス中に、認証シーケンスを含めることによって、IPアドレスの移動に係る制御と同時に認証処理を行うことが可能となり、位置登録シーケンスと認証シーケンスが独立に行われていた場合に比べて、ハンドオーバに要する時間が短縮し、移動端末21に対してシームレスな接続サービスを提供することが可能となる。

(第2の実施の形態)

次に、図面を参照しながら、本発明の第2の実施の形態について説明する。本発明の第2の実施の形態では、HMI P v 6の位置登録シーケンス中に認証シーケンスを含め、さらに、認証処理にかかる時間（認証時間）を考慮して、その認証時間中においても、移動端末21がネットワークにアクセスできるようにすることによって、ハンドオーバに要する時間を短縮し、シームレスな接続サービスを提供することを可能とする技術について説明する。

これは、特に、アクセスを提供しているオペレータ30に属するアクセスネットワークと利用者のオペレータ40に属するホームネットワークとが異なっており、MAP 10が認証サーバ32、42に対して認証依頼を行ってから認証結果が返ってくるまでの時間が長い場合に有効である。このように認証時間が長くなる理由は、アクセスネットワークとホームネットワークとが離れていることに加え、以下の理由による。

移動端末 21 がアクセスネットワークに接続するためには、まず、アクセスネットワークとホームネットワークとが、互いにローミング契約をしている必要があるが、この場合、移動端末 21 はアクセスネットワークにとってはローミング端末となるため、アクセスネットワーク内の
5 認証サーバ 32 が当該移動端末 21 の認証情報を有さないことがある。この場合、通常、アクセスを提供しているオペレータ 30 に属する認証サーバ 32（アクセスネットワーク上の認証サーバ 32）が利用者のオペレータ 30 に属する認証サーバ 42（ホームネットワーク上の認証サーバ 42）に対して移動端末 21 の認証依頼を行う。なお、このような
10 認証情報転送機構は、各オペレータ間のローミング契約や認証サーバ間のプロトコルなどに依存するものである。

図 3 は、本発明の第 2 の実施の形態における MAP の構成を示すブロック図である。図 3 に示す MAP 10 は、上位ネットワーク 20 と接続する上位ネットワーク通信手段 11、下位ネットワーク 25 と接続する
15 下位ネットワーク通信手段 12、HMI Pv 6 を利用したデータ伝送の経路を決定及び制御する HMI Pv 6 経路制御手段 13、認証サーバ 32 に対して認証要求の送信及び認証結果の受信を行う認証要求送受信手段 14、データ伝送経路の設定の際に参照される HMI Pv 6 テーブル（RCOA/LCOA テーブルを含む）16、認証サーバ 32 のアドレ
20 ス 17、状態テーブル 19 を格納する情報格納手段 15、時間管理手段 18 を有している。

このうち、本発明の第 1 の実施の形態に加えて特徴的な構成要素は時間管理手段 18 と、情報格納手段 15 に格納された状態テーブル 19 であり、上位ネットワーク通信手段 11、下位ネットワーク通信手段 12、
25 HMI Pv 6 経路制御手段 13、認証要求送受信手段 14 は、本発明の第 1 の実施の形態で存在するものを利用することが可能である。なお、

MAP 10はコンピュータによって実現可能であり、上記の各手段はCPUなどの中央処理手段によって実現可能であるとともに、様々な情報の参照し、判断・判定処理を行うことも可能である。

時間管理手段18は、主に、時間を計測する計時機能と、計時結果に
5 従って所定の値を減算（後述の図6に示す状態テーブル19中の設定値をスタート値とするカウントダウン）し、残り時間が0になったか否かを判定する残り時間判定機能を有している。また、様々な時間情報の設定を行う時間設定手段としての機能も有している。なお、所定の時間が経過したか否かの判定が可能であれば、残り時間判定機能のほかに、所
10 定の時間が経過したか否かを判定する機能、又は、所定の時刻に達したか否かを判定する機能を用いることも可能である。

図4は、本発明の第2の実施の形態におけるシーケンスを示す図である。図4には、図2と同様、移動端末21、アクセスを提供しているオペレータ30、利用者のオペレータ40が図示されており、アクセスを
15 提供しているオペレータ30には、アクセスルータ31、MAP 10、認証サーバ32が存在し、利用者のオペレータ40には、ホームページ41、認証サーバ42が存在する。なお、図4におけるMAP 10は、図3に示す本発明を実施するためのMAP 10である。

第1の実施の形態と同様、移動端末21が新たなリンクに接続した場合、移動端末21はアクセスルータに対して、ルータソリシテーションを送信し（ステップS201）、これを受けて、アクセスルータは移動
20 端末21に対して、ルータアドバタイズメントを送信する（ステップS202）。そして、移動端末21は、アクセスルータからのルータアドバタイズメントを受けて、接続したリンク上のLCOAとMAP 10のアドレスとを取得し、RCOAを構成する。
25

次に、HMIPv6を実装する移動端末21は、MAP 10への

Binding Updateを行うため、L C o Aと、端末I D及び利用者情報を含む認証情報とを、M A P 1 0に対して送信する（ステップS 2 0 3）。M A P 1 0は、このBinding Updateに関してR C o A及びL C o Aの登録を行い、移動端末2 1に対して、十分に短い接続の有効時間（仮Binding
5 有効時間T 1）を設定してBinding Acknowledgementを返信する（ステップS 2 0 4）。なお、このBinding Acknowledgementは、仮Binding有効時間T 1だけネットワークへの接続許可を与えるものであり、すなわち、このBinding Acknowledgementを受けた移動端末2 1は、仮Binding有効時間T 1だけネットワークに接続することが可能となる。

10 さらに、M A P 1 0は、情報格納手段1 5内に格納されている認証サーバ3 2のアドレス1 7を参照し、認証要求送受信手段1 4を用いて、認証サーバ3 2に対して認証要求を送信する（ステップS 2 0 5）。また、必要ならば、アクセスを提供しているオペレータ3 0の認証サーバ3 2は、利用者のオペレータ4 0の認証サーバ4 2に対して認証依頼を
15 送信し（ステップS 2 0 6）、認証処理後の応答（認証結果）を受信する（ステップS 2 0 7）。そして、認証サーバ3 2はM A P 1 0に対して、認証結果を返す（ステップS 2 0 8）。

なお、第1の実施の形態と同様、上記のステップS 2 0 6及びステップS 2 0 7の処理が必要でない場合（アクセスを提供しているオペレー
20 タ3 0の認証サーバ3 2において、認証処理が可能な場合）には、アクセスを提供しているオペレータ3 0の認証サーバ3 2で認証処理を行って、その認証結果をM A P 1 0に返すようにする。また、M A P 1 0が、利用者のオペレータ4 0の認証サーバ4 2と認証依頼及び認証結果のやり取りを直接行うことも可能である。

25 一方、M A P 1 0は、仮Binding有効時間T 1だけネットワークへの接続が許可された後も、周期的又は仮Binding有効時間T 1に達する直前に

、MAP 10へのBinding Updateを行うための情報（L C o A）と、端末ID及び利用者情報を含む認証情報とを、MAP 10に対して送信する（ステップS 209）。

- このステップS 209におけるBinding Updateを受けた時点で、ステップS 208における認証サーバ32からの認証結果の受信が完了している場合には、MAP 10は、Binding Acknowledgementと認証結果とを移動端末21に対して送信する（ステップS 210）。このとき、認証結果が成功を示すものである場合には、MAP 10は、移動端末21に対して、接続許可及び仮Binding有効時間T 1に比べて十分長いBinding有効時間T 2を送信する。このBinding Acknowledgementを受けた移動端末21は、Binding有効時間T 2だけネットワークに接続することが可能となる。その後は、従来と同様のHMIP v 6におけるホームエージェント41へのBinding Updateが行われ、移動端末21がR C o Aをホームエージェント41に送信し、ホームエージェント41から登録完了を示す
- 10 Binding Acknowledgementを受信する。

- 一方、図4には不図示だが、ステップS 209におけるBinding Updateを受けた時点で、ステップS 208における認証サーバ32からの認証結果の受信が完了していない場合（認証結果の受信前に移動端末21からBinding Updateを再受信した場合）には、MAP 10は、再びステップS 204に戻り、移動端末21に対して仮Binding有効時間T 1だけネットワークへの接続許可を与えるBinding Acknowledgementを送信する。
- 20 なお、移動端末21に対して仮Binding有効時間T 1だけネットワークへの接続許可を与えるBinding Acknowledgementを送信する処理は、認証サーバ32から認証結果を受信するまで繰り返される。

- 25 さらに、図4には不図示だが、所定の認証要求有効時間T aが経過しても、認証サーバ32から認証結果を受信することができなかった場合

(すなわち、ステップ S 2 0 8 の処理が行われなかった場合) には、M A P 1 0 は、当該移動端末 2 1 の認証が失敗したとみなして、移動端末 2 1 に対して認証失敗を示す認証結果を送信するとともに、所定の認証要求再開時間 T r の間は接続禁止期間 (接続禁止時間) とし、当該移動
5 端末 2 1 からの Binding Update に対して、接続禁止期間であることを示す Binding Acknowledgement を返すようにする。

また、上記のシーケンスにおいて、移動端末 2 1 から Binding Update を受けた際の M A P 1 0 の処理の詳細について説明する。図 5 は、本発明の第 2 の実施の形態における移動端末から Binding Update を受けた際
10 の M A P の処理の詳細を示すフローチャートである。M A P 1 0 は、移動端末 2 1 から Binding Update を受信し (ステップ S 3 0 1)、状態テーブル 1 9 に当該 Binding Update の送信元の移動端末 2 1 の L C o A が存在しているか否かを調べる (ステップ S 3 0 2)。

また、図 6 は、本発明の第 2 の実施の形態における状態テーブルの一
15 例を示す模式図である。図 6 に示されているように、状態テーブル 1 9 には、移動端末 2 1 の L C o A、認証結果、認証要求有効時間 T a の設定値、認証要求再開時間 T r の設定値、仮 Binding 時間 T 1 の設定値、Binding 時間 T 2 の設定値の組み合わせが記録される。なお、認証結果は、この移動端末 2 1 の認証処理における状態や認証結果を含むものであ
20 り、例えば、現在認証処理中であることを示す「処理中」、認証に成功したことを示す「認証成功」、認証に失敗したことを示す「認証失敗」、接続が禁止されていることを示す「禁止」などが挙げられる。また、仮 Binding 時間 T 1 及び認証要求有効時間 T a は認証処理中の状態で付与されるもの、Binding 時間 T 2 は認証成功の状態で付与されるもの、認証
25 要求再開時間 T r は認証失敗の状態で付与されるものである。

この移動端末 2 1 の L C o A が状態テーブル 1 9 に存在していない場

合には、この移動端末 21 の LC o A を状態テーブル 19 に加えて（ステップ S 303）、状態テーブル 19 中の当該 LC o A の認証結果を「処理中」にセットする（ステップ S 304）。そして、当該 BU 中の認証情報（移動端末 21 の端末 ID や利用者情報）を基にして、この移動
5 端末 21 の認証処理を行うよう要求する認証要求を認証サーバ 32 に送信し（ステップ S 305）、同時に、当該 LC o A の認証要求有効時間 Ta をセットし、カウントダウン（減算処理）を開始する（ステップ S 306）。

なお、認証要求有効時間 Ta として、認証サーバ 32 とのやり取りや
10 認証サーバ 32 での認証処理にかかる時間より少し長い時間が設定されることが好ましい。また、移動端末 21 や認証サーバ 32 に係る様々な条件を考慮して、認証要求有効時間 Ta を移動端末 21 毎（LC o A 毎）に設定することも可能であり、一律に所定の値に設定することも可能である。

15 そして、RC o A / LC o A テーブルに、この移動端末 21 の RC o A / LC o A の組を追加（登録）し（ステップ S 307）、当該 LC o A の仮Binding時間 T1 をセットし、カウントダウン（減算処理）を開始する（ステップ S 308）。なお、仮Binding時間 T1 として、その時間内では不正なネットワークアクセスが不可能な程度に短い時間が設定さ
20 れることが好ましい。また、移動端末 21 や認証サーバ 32 に係る様々な条件を考慮して、仮Binding時間 T1 を移動端末 21 毎（LC o A 毎）に設定することも可能であり、一律に所定の値に設定することも可能である。このようにして設定された接続許可と、接続が許可される有効時間である仮Binding時間 T1 とを記載した Binding Acknowledgement を当
25 該移動端末 21 に送信し（ステップ S 309）、移動端末 21 や認証サーバ 32 からの応答を受信したり、認証要求有効時間 Ta や仮Binding

時間 T 1 のカウントダウンが 0 になったりする場合まで、待機状態となる。

- 一方、この移動端末 2 1 の L C o A が状態テーブル 1 9 に存在している場合には、当該 L C o A の認証結果が「処理中」であるか否かを調べる（ステップ S 3 1 0）。当該 L C o A の認証結果が「処理中」である場合には、Binding Acknowledgement 内に「処理中」であることを記載し（ステップ S 3 1 1）、当該 L C o A の仮 Binding 時間 T 1 をセットし、新たにカウントダウン（減算処理）を開始して（ステップ S 3 1 2）、新たに設定された接続許可と、接続が許可される有効時間である仮
- 10 Binding 時間 T 1 とを記載した Binding Acknowledgement を当該移動端末 2 1 に送信する（ステップ S 3 1 3）。そして、移動端末 2 1 や認証サーバ 3 2 からの応答を受信したり、認証要求有効時間 T a や仮 Binding 時間 T 1 のカウントダウンが 0 になったりする場合まで、待機状態となる。
- 15 また、当該 L C o A の認証結果が「処理中」でない場合には、当該 L C o A の認証結果が「禁止」であるか否かを調べる（ステップ S 3 1 4）。当該 L C o A の認証結果が「禁止」である場合には、Binding Acknowledgement 内に、接続禁止期間であることを記載して、移動端末 2 1 に送信する（ステップ S 3 1 5）。
- 20 また、当該 L C o A の認証結果が「禁止」でない場合には、当該 L C o A の認証結果が「認証成功」であるか否かを調べる（ステップ S 3 1 6）。当該 L C o A の認証結果が「認証成功」である場合には、R C o A / L C o A テーブルに、この移動端末 2 1 の R C o A / L C o A の組を追加（登録）し（ステップ S 3 1 7）、当該 L C o A の Binding 時間 T
- 25 2 をセットし、カウントダウン（減算処理）を開始する（ステップ S 3 1 8）。なお、Binding 時間 T 2 として、移動端末 2 1 に十分な接続サー

ビスを提供できる程度に長い時間が設定されることが好ましい。また、移動端末 2 1 や認証サーバ 3 2 に係る様々な条件を考慮して、Binding 時間 T 2 を移動端末 2 1 毎(L C o A 毎)に設定することも可能であり、一律に所定の値に設定することも可能である。MAP 1 0 は、このよう
5 にして設定された接続許可と、接続が許可される有効時間であるBinding 時間 T 2 とを記載したBinding Acknowledgementを当該移動端末 2 1 に送信し(ステップ S 3 1 9)、移動端末 2 1 に対して、Binding 時間 T 2 の接続サービスを提供する。

また、当該 L C o A の認証結果が「認証成功」でない場合には、当該
10 L C o A の認証結果は「認証失敗」とみなされ、Binding Acknowledgement内に、認証失敗であることを記載して、移動端末 2 1 に送信する(ステップ S 3 2 0)。また、所定の時間(認証要求再開時間 T r)だけの期間、その移動端末 2 1 の認証処理を行わないようにするため、状態テーブル 1 9 中の当該移動端末 2 1 の L C o A の認証結果を
15 「禁止」にセットし(ステップ S 3 2 1)、同時に、当該 L C o A の認証要求再開時間 T r をセットし、カウントダウン(減算処理)を開始する(ステップ S 3 2 2)。

図 5 に示すフローチャートでは、MAP 1 0 は、所定の処理を終了して待機状態となる。この待機状態では、MAP 1 0 は、移動端末 2 1 や
20 認証サーバ 3 2 からの応答の受信を待機する状態、仮Binding時間 T 1、Binding 時間 T 2、認証要求有効時間 T a、認証要求再開時間 T r のカウントダウンが 0 になるまで待機する状態など、様々な待機状態となっている。この待機状態中に再び移動端末 2 1 から B U を受信した場合には、図 5 に示すフローチャートに示す処理を繰り返す一方、認証サーバ 3 2
25 から認証結果を受信した場合や仮Binding時間 T 1、Binding 時間 T 2、認証要求有効時間 T a、認証要求再開時間 T r のカウントダウンが 0 に

なった場合には、図 7 に示すフローチャートの処理を行う。

図 7 は、本発明の第 2 の実施の形態における認証サーバから認証結果を受信した場合及び所定の時間が経過した場合の MAP の処理の詳細を示すフローチャートである。なお、図 7 に示すフローチャートは、図 5 に示すフローチャートから連続したものであり、図 5 に示す待機状態（ステップ S 3 3 3）と図 7 に示す待機状態（ステップ S 3 3 3）は同一ステップである。

まず、MAP 10 が、認証サーバ 3 2 から移動端末 2 1 の認証結果を受信（ステップ S 3 4 1）した場合、状態テーブル 1 9 中にその認証処理の対象となった移動端末 2 1 が存在しているか否か（当該移動端末 2 1 に係るエントリが存在しているか否か）を調べる（ステップ S 3 4 2）。当該移動端末 2 1 が存在していない場合には、すでにその移動端末 2 1 に係る認証処理を行う必要はなく、再び待機状態に戻る。一方、当該移動端末 2 1 が存在する場合には、認証結果が許可を示すものか否かを判定する（ステップ S 3 4 3）。

認証結果が許可を示すものであった場合には、MAP 10 は、状態テーブル 1 9 中の当該移動端末 2 1 の認証結果を「認証成功」に設定し（ステップ S 3 4 4）、認証成功の場合の処理（ステップ S 3 1 7～S 3 1 9 までの処理と同一）を行う（ステップ S 3 4 5）一方、認証結果が不許可を示すものであった場合には、MAP 10 は、状態テーブル 1 9 中の当該移動端末 2 1 の認証結果を「認証失敗」に設定し（ステップ S 3 4 6）、認証失敗の場合の処理（ステップ S 3 2 0～S 3 2 2 までの処理と同一）を行って（ステップ S 3 4 7）、再び待機状態に戻る。

また、認証要求再開時間 T_r が 0 になった（ステップ S 3 4 8）場合には、その移動端末 2 1 に対する接続禁止区間の設定を終了し、状態テーブル 1 9 中から、その移動端末 2 1 に係るエントリを削除する（ステ

ップS 3 4 9)。また、認証要求有効時間T a が0になった（ステップS 3 5 0）場合には、認証サーバ3 2から認証結果を取得することができず、状態テーブル1 9中の当該移動端末2 1の認証結果を「認証失敗」に設定し（ステップS 3 5 1）、認証失敗の場合の処理（ステップS 3 2 0～S 3 2 2までの処理と同一）を行って（ステップS 3 5 2）、再び待機状態に戻る。

また、仮Binding時間T 1又はBinding時間T 2が0になった（ステップS 3 5 3）場合には、その移動端末2 1に提供している接続サービスの有効期限が切れて無効になったとみなし、R C o A / L C o Aテーブルから当該移動端末2 1に関する情報を削除して（ステップS 3 5 4）、再び待機状態に戻る。

以上、説明したように、本発明の第2の実施の形態によれば、シームレスハンドオーバを目的とし、すでに標準化が進められているH M I P v 6の位置登録シーケンス中に認証シーケンスを含め、さらに、認証シーケンスに時間がかかる場合を考慮して、その認証時間中においても、移動端末2 1がネットワークにアクセスできるようにすることによって、I Pアドレスの移動に係る制御と同時に認証処理を行うことが可能となり、位置登録シーケンスと認証シーケンスが独立に行われていた場合や本発明の第1の実施の形態で説明した位置登録シーケンスと認証シーケンスとを同時に行う技術に比べて、さらに、ハンドオーバに要する時間が短縮し、移動端末2 1に対してシームレスな接続サービスを提供することが可能となる。

また、上記の第2の実施の形態では、特にH M I P v 6を利用する無線通信システムを例にして説明したが、下記の1～4に示す

1. 短時間だけ仮の接続許可を与えること（上記の仮Binding時間T 1に対応）

2. 接続許可に時間制限を設けること（上記のBinding時間T₂に対応）

3. 認証サーバに認証要求を行う際にその応答を受けるまでの時間を設定すること（上記の認証要求有効時間T_aに対応）

5 4. 認証に失敗した移動端末に対しては、一定時間だけ接続を禁止すること（上記の認証要求再開時間T_rに対応）

は、HMIPv6に限らず、例えば、グローバルIPv4や、従来の技術で説明したDiameter Mobile IPv4など、他の通信プロトコルを利用する無線通信システムにおいても適用可能である。

10 この場合、上記の第2の実施の形態において、MAP10を管理サーバ、Binding Updateを接続要求、Binding Acknowledgementを接続要求への応答、Binding時間を接続許可時間、LCoAを端末識別情報、RCoA/LCoAテーブルを接続許可テーブルなどとそれぞれ読み換え、状態テーブルとして、図8に示す状態テーブルを用いることにより、HMIPv6
15 以外の通信プロトコルへの一般化が可能である。また、上記の第2の実施の形態では、管理サーバが、認証に成功した移動端末21に対して、すぐに接続サービスを提供するようにしているが、移動端末21からの接続要求があってその認証に成功した場合、まず、状態テーブルに「認証成功」の旨を記載しておき、次に、再び当該移動端末から接続要求を受信した場合に、状態テーブルの「認証成功」の記載を確認して、初め
20 て通常の時間の接続サービスを提供することも可能である。

産業上の利用可能性

以上、説明したように、本発明によれば、HMIPv6を用いて移動
25 端末のリンク接続を管理する無線通信システムにおける無線通信管理方法に関し、移動端末のリンク接続を管理するサーバに対して、移動端末

が、リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を送信し、位置登録シーケンスと認証シーケンスとを同時に行えるようにしているので、移動端末がリンク接続を変更するハンドオーバー時に、スムーズにハンドオーバーを行えるよう

5 うにするとともに、リンク接続の変更に要する時間を短縮することが可能となる。

請 求 の 範 囲

1. HMI P v 6 を用いて移動端末のリンク接続を管理する無線通信システムにおける無線通信管理方法であって、
- 5 前記移動端末の前記リンク接続を管理するサーバに対して、前記移動端末が、前記リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を送信し、前記移動端末の前記リンク接続の変更に要する時間を短縮する無線通信管理方法。
- 10 2. 前記移動端末が、前記リンク接続を変更するための情報と、前記認証に係る情報とを1つの情報として送信し、前記リンク接続を管理するサーバが、前記1つの情報から、前記リンク接続を変更するための情報及び前記認証に係る情報のそれぞれを取得する請求項1に記載の無線通信管理方法。
- 15 3. 前記リンク接続を管理するサーバが、前記認証に係る情報を用いた認証処理による認証結果を取得する請求項1に記載の無線通信管理方法。
- 20 4. 前記リンク接続を管理するサーバが、前記移動端末の認証を行う認証サーバとの通信を行い、前記認証結果を取得する請求項3に記載の無線通信管理方法。
5. 前記移動端末の前記リンク接続の変更を確認した旨を通知する情報と、前記認証結果とを1つの情報として、前記移動端末に送信する請求項3に記載の無線通信管理方法。
- 25

6. 前記リンク接続を管理するサーバが、前記移動端末の前記リンク接続の変更を確認した旨を通知する情報を前記移動端末に送信し、その後、前記認証結果を取得できた場合に前記認証結果を前記移動端末に送信する請求項3に記載の無線通信管理方法。

5

7. 前記リンク接続を管理するサーバが、前記認証結果の取得までの時間を設定し、前記認証結果の取得までの時間内に前記認証結果を取得できた場合、次に前記移動端末から前記リンク接続を変更するための情報を受信した際に、前記移動端末の前記リンク接続の変更を確認した旨を通知する情報と共に、前記認証結果を前記移動端末に送信する請求項6に記載の無線通信管理方法。

10

8. 前記リンク接続を管理するサーバが、前記移動端末が前記所望のネットワークへのアクセスを仮許可する所定の仮許可時間を設定し、前記移動端末の前記リンク接続の変更を確認した旨を通知する情報と共に、前記所定の時間だけ前記所望のネットワークへのアクセスの許可を通知する情報を前記移動端末に送信する請求項7に記載の無線通信管理方法。

15

20 9. 前記リンク接続を管理するサーバが、前記所定の仮許可時間よりも長い時間であって、前記移動端末が前記所望のネットワークへのアクセスを許可する所定の許可時間を設定し、前記認証結果が認証成功であった場合、前記移動端末の前記リンク接続の変更を確認した旨を通知する情報と共に、所定の許可時間だけ前記所望のネットワークへのアクセスの許可を通知する情報を前記移動端末に送信する請求項8に記載の無線通信管理方法。

25

10. 前記リンク接続を管理するサーバが、前記所定の仮許可時間又は前記所定の許可時間だけ前記所望のネットワークへのアクセスを許可した前記移動端末の前記リンク接続の変更に係る登録を行い、前記所定の仮許可時間又は前記所定の許可時間が経過した場合、前記移動端末
- 5 の前記リンク接続の変更に係る登録を削除する請求項8に記載の無線通信管理方法。
11. 前記リンク接続を管理するサーバが、前記認証結果の取得までの時間を設定し、前記認証結果の取得までの時間内に前記認証結果を
- 10 取得できなかった場合、前記認証結果を認証失敗とする請求項3に記載の無線通信管理方法。
12. 前記リンク接続を管理するサーバが、前記移動端末に対して所定の接続禁止時間を設定し、前記移動端末に対して前記認証結果として認証失敗を通知した場合には、前記認証失敗の通知から前記所定の接続禁止時間だけ、前記認証失敗であった前記移動端末の前記リンク接続
- 15 の変更に係る処理及び前記認証に係る処理を行わないようにする請求項5又は6に記載の無線通信管理方法。
13. 前記リンク接続を管理するサーバが、前記移動端末に対して前記認証結果として認証成功を通知した場合のみ、前記認証成功であった前記移動端末の前記リンク接続の変更に係る登録を行うようにする請求項5又は6に記載の無線通信管理方法。
- 20 14. 移動端末のリンク接続を管理する無線通信システムにおける無線通信管理方法であって、
- 25

前記移動端末の前記リンク接続を管理するサーバに対して、前記移動端末が、前記リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を送信し、

- 5 前記リンク接続を管理するサーバが、前記認証に係る情報を用いた認証処理による認証結果の取得までの時間を設定し、前記認証結果の取得までの時間内に前記認証結果を取得できた場合、前記認証結果を前記移動端末に送信する無線通信管理方法。

- 10 15. 前記リンク接続を管理するサーバが、前記移動端末が前記所望のネットワークへのアクセスを仮許可する所定の仮許可時間を設定し、前記所定の時間だけ前記所望のネットワークへのアクセスの許可を通知する情報を前記移動端末に送信する請求項14に記載の無線通信管理方法。

- 15 16. 前記リンク接続を管理するサーバが、前記所定の仮許可時間よりも長い時間であって、前記移動端末が前記所望のネットワークへのアクセスを許可する所定の許可時間を設定し、前記認証結果が認証成功であった場合、所定の許可時間だけ前記所望のネットワークへのアクセスの許可を通知する情報を前記移動端末に送信する請求項15に記載の無線通信管理方法。

- 25 17. 前記所定の仮許可時間又は前記所定の許可時間が経過した場合、前記リンク接続を管理するサーバは、前記移動端末の前記接続を切断する請求項15又は16に記載の無線通信管理方法。

18. 移動端末のリンク接続を管理する無線通信システムにおける

無線通信管理方法であって、

前記移動端末の前記リンク接続を管理するサーバに対して、前記移動端末が、前記リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を送信し、

- 5 前記リンク接続を管理するサーバが、前記認証に係る情報を用いた認証処理による認証結果の取得までの時間を設定し、前記認証結果の取得までの時間内に前記認証結果を取得できなかった場合、前記認証結果を認証失敗とする無線通信管理方法。

- 10 19. 前記リンク接続を管理するサーバが、前記移動端末に対して所定の接続禁止時間を設定し、前記移動端末に対して前記認証結果として認証失敗を通知した場合には、前記認証失敗の通知から前記所定の接続禁止時間だけ、前記認証失敗であった前記移動端末に係る処理を行わないようにする請求項14又は18に記載の無線通信管理方法。

15

20. 前記リンク接続を管理するサーバが、前記移動端末に対して前記認証結果として認証成功を通知した場合のみ、前記認証成功であった前記移動端末の前記リンク接続の変更に係る登録を行うようにする請求項14に記載の無線通信管理方法。

20

21. HMI P v 6 を用いて移動端末のリンク接続を管理する無線通信管理サーバであって、

- 前記移動端末から、前記リンク接続を変更するための情報と所望のネットワークにアクセスするための認証に係る情報とを1つの情報で受信
25 し、前記1つの情報から、前記リンク接続を変更するための情報及び前記認証に係る情報のそれぞれを取得するよう構成されている無線通信管

理サーバ。

22. 前記認証に係る情報を用いた認証処理による認証結果を取得するよう構成されている請求項21に記載の無線通信管理サーバ。

5

23. 前記移動端末の認証を行う認証サーバとの通信を行う手段を有し、

前記認証結果を取得するよう構成されている請求項22に記載の無線通信管理サーバ。

10

24. 前記移動端末の前記リンク接続の変更を確認した旨を通知する情報と前記認証結果とを1つの情報として、前記移動端末に送信するよう構成されている請求項22に記載の無線通信管理サーバ。

15 25. 前記移動端末の前記リンク接続の変更を確認した旨を通知する情報を前記移動端末に送信し、その後、前記認証結果を取得できた場合に前記認証結果を前記移動端末に送信するよう構成されている請求項22に記載の無線通信管理サーバ。

20 26. 前記認証結果の取得までの時間を設定する時間設定手段を有し、前記認証結果の取得までの時間内に前記認証結果を取得できた場合、
前記移動端末から前記リンク接続を変更するための情報を受信した際に、前記移動端末の前記リンク接続の変更を確認した旨を通知する情報と共に、前記認証結果を前記移動端末に送信するよう構成されている
25 請求項25に記載の無線通信管理サーバ。

27. 前記移動端末に対して前記所望のネットワークへのアクセスを仮許可する所定の仮許可時間を設定する時間設定手段を有し、

前記移動端末の前記リンク接続の変更を確認した旨を通知する情報と共に、前記所定の時間だけ前記所望のネットワークへのアクセスの許可を通知する情報を前記移動端末に送信するよう構成されている請求項26に記載の無線通信管理サーバ。

28. 前記移動端末に対して、前記所定の仮許可時間よりも長い時間であって、前記移動端末が前記所望のネットワークへのアクセスを許可する所定の許可時間を設定する時間設定手段を有し、

前記認証結果が認証成功であった場合、前記移動端末の前記リンク接続の変更を確認した旨を通知する情報と共に、所定の許可時間だけ前記所望のネットワークへのアクセスの許可を通知する情報を前記移動端末に送信するよう構成されている請求項27に記載の無線通信管理サーバ。

29. 前記所定の仮許可時間又は前記所定の許可時間だけ前記所望のネットワークへのアクセスを許可した前記移動端末の前記リンク接続の変更に係る登録を行う情報登録手段と、

前記所定の仮許可時間又は前記所定の許可時間が経過した場合、前記移動端末の前記リンク接続の変更に係る登録を削除する情報削除手段とを、

有する請求項27に記載の無線通信管理サーバ。

30. 前記認証結果の取得までの時間を設定する時間設定手段と、

前記認証結果の取得までの時間内に前記認証結果を取得できなかった場合、前記認証結果を認証失敗とする判定手段とを、

有する請求項 2 2 に記載の無線通信管理サーバ。

3 1. 前記移動端末に対して所定の接続禁止時間を設定する時間設定手段と、

- 5 前記移動端末に対して前記認証結果として認証失敗を通知した場合には、前記認証失敗の通知から前記所定の接続禁止時間だけ、前記認証失敗であった前記移動端末の前記リンク接続の変更に係る処理及び前記認証に係る処理を行わないよう制御する制御手段とを、

有する請求項 2 4 又は 2 5 に記載の無線通信管理サーバ。

10

3 2. 前記移動端末に対して前記認証結果として認証成功を通知した場合のみ、前記認証成功であった前記移動端末の前記リンク接続の変更に係る登録を行うよう制御する制御手段を有する請求項 2 4 又は 2 5 に記載の無線通信管理サーバ。

15

3 3. 移動端末のリンク接続を管理する無線通信管理サーバであって、

前記移動端末から、前記リンク接続を変更するための情報と同時に、
所望のネットワークにアクセスするための認証に係る情報を受信する受
20 信手段と、

前記認証に係る情報を用いた認証処理による認証結果の取得までの時間を設定する時間設定手段と、

前記認証結果の取得までの時間内に前記認証結果を取得できた場合、
前記認証結果を前記移動端末に送信する送信手段とを、

- 25 有する無線通信管理サーバ。

34. 前記移動端末が前記所望のネットワークへのアクセスを仮許可する所定の仮許可時間を設定する時間設定手段を有し、

前記所定の時間だけ前記所望のネットワークへのアクセスの許可を通知する情報を前記移動端末に送信するよう構成されている請求項33に記載の無線通信管理サーバ。

35. 前記所定の仮許可時間よりも長い時間であって、前記移動端末が前記所望のネットワークへのアクセスを許可する所定の許可時間を設定する時間設定手段を有し、

10 前記認証結果が認証成功であった場合、所定の許可時間だけ前記所望のネットワークへのアクセスの許可を通知する情報を前記移動端末に送信するよう構成されている請求項34に記載の無線通信管理サーバ。

36. 前記所定の仮許可時間又は前記所定の許可時間が経過した場合、前記移動端末の前記接続を切断する制御手段を有する請求項34又は35に記載の無線通信管理サーバ。

37. 移動端末のリンク接続を管理する無線通信システムにおける無線通信管理サーバであって、

20 前記移動端末から、前記リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を受信する受信手段と、

前記リンク接続を管理するサーバが、前記認証に係る情報を用いた認証処理による認証結果の取得までの時間を設定する時間設定手段と、

25 前記認証結果の取得までの時間内に前記認証結果を取得できなかった場合、前記認証結果を認証失敗として、前記認証結果を前記移動端末に

送信する送信手段とを、

有する無線通信管理サーバ。

38. 前記移動端末に対して所定の接続禁止時間を設定する時間設定手段と、

前記移動端末に対して前記認証結果として認証失敗を通知した場合には、前記認証失敗の通知から前記所定の接続禁止時間だけ、前記認証失敗であった前記移動端末に係る処理を行わないよう制御する制御手段とを、

- 10 有する請求項33又は37に記載の無線通信管理サーバ。

39. 前記移動端末に対して前記認証結果として認証成功を通知した場合のみ、前記認証成功であった前記移動端末の前記リンク接続の変更に係る登録を行うよう制御する制御手段を有する請求項33に記載の

- 15 無線通信管理サーバ。

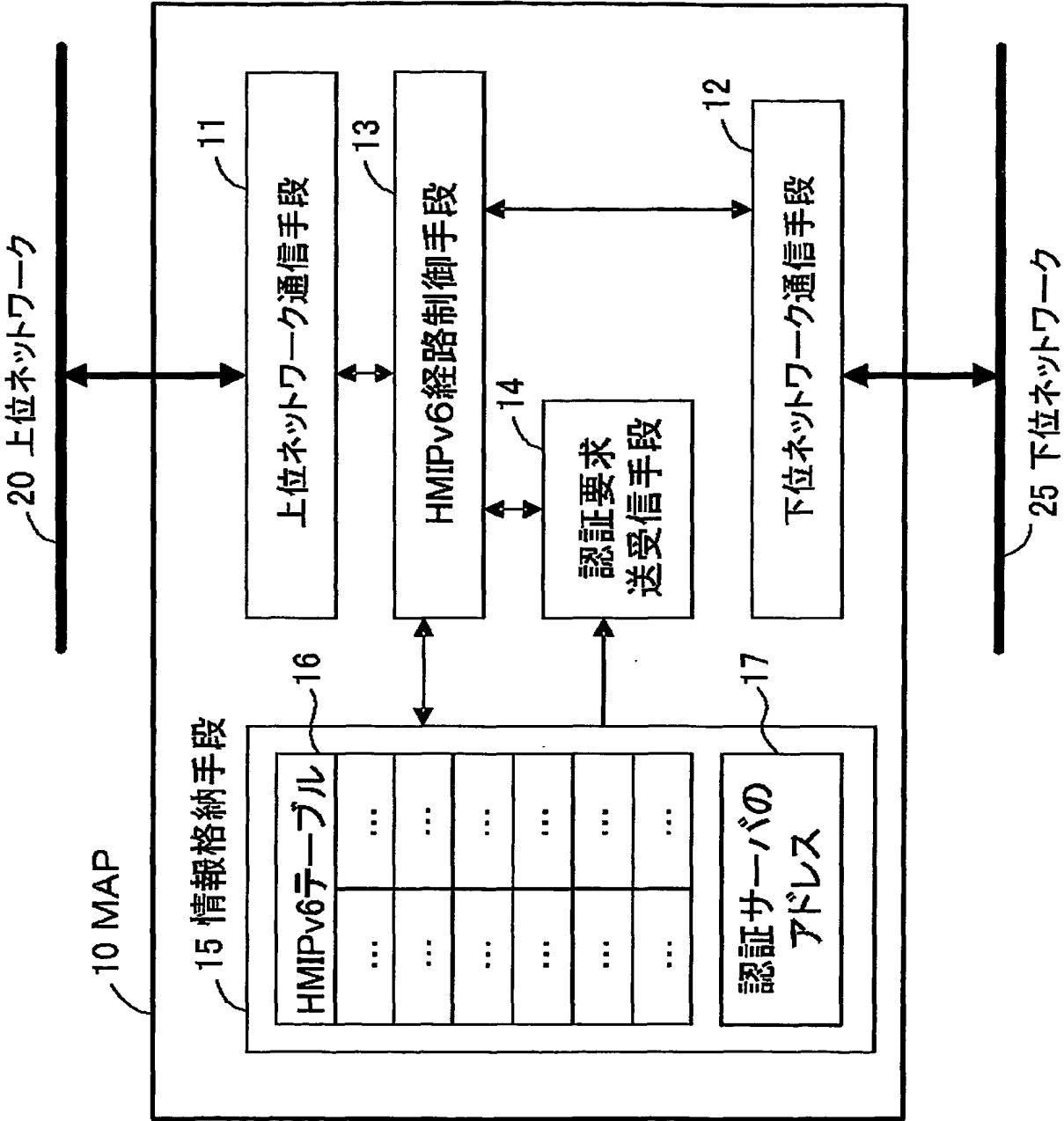


FIG. 1

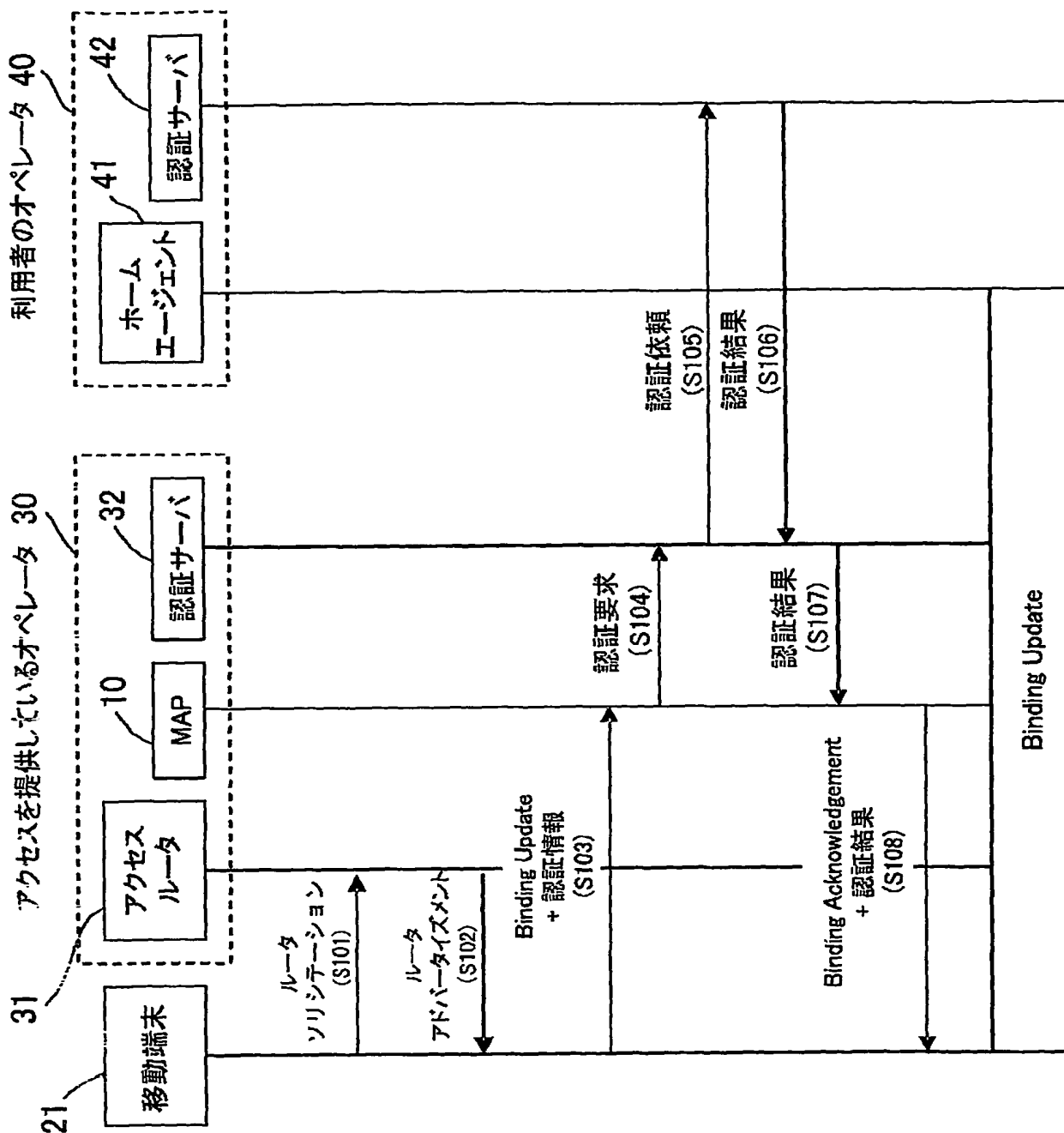


FIG. 2

FIG. 3

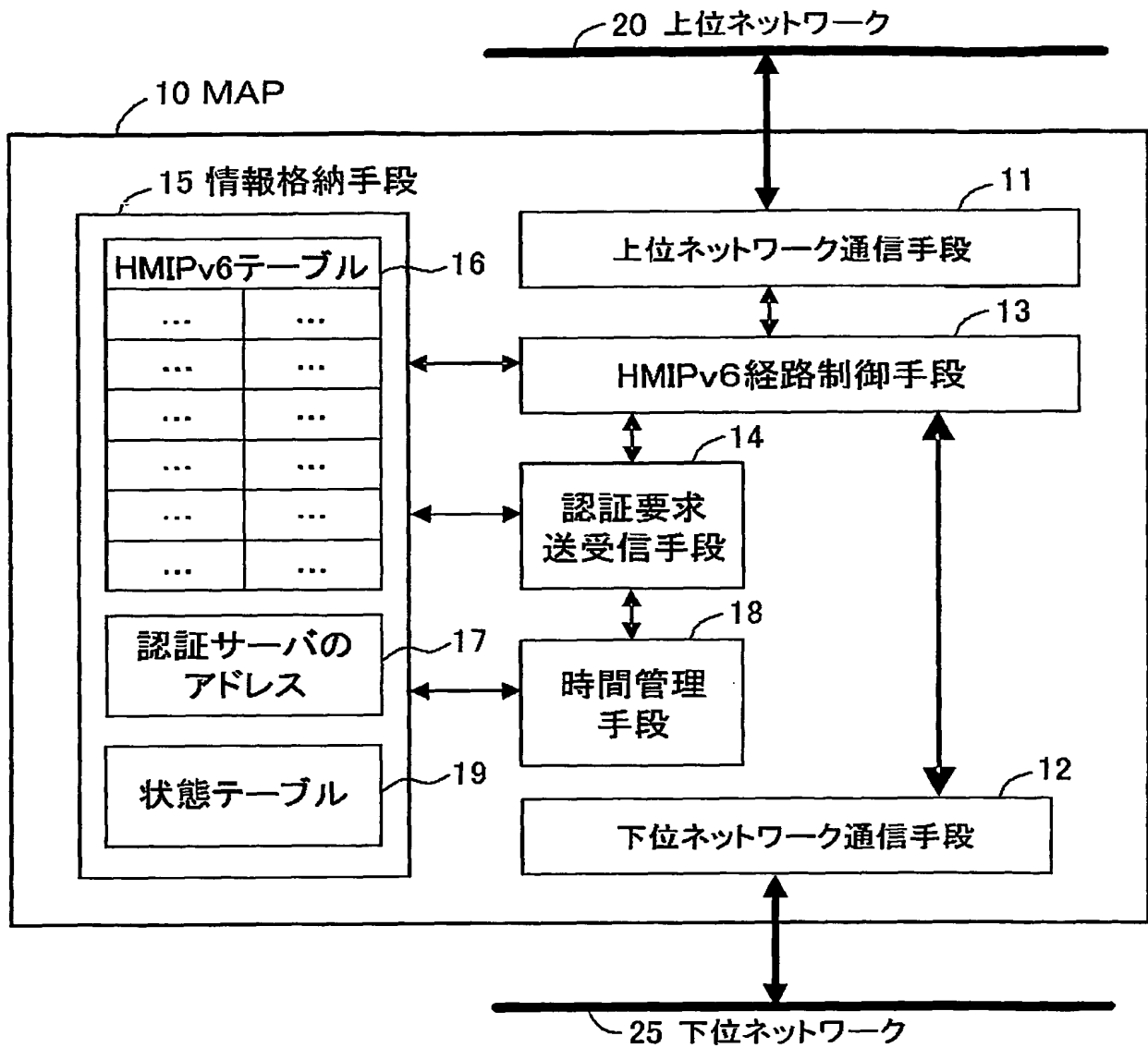
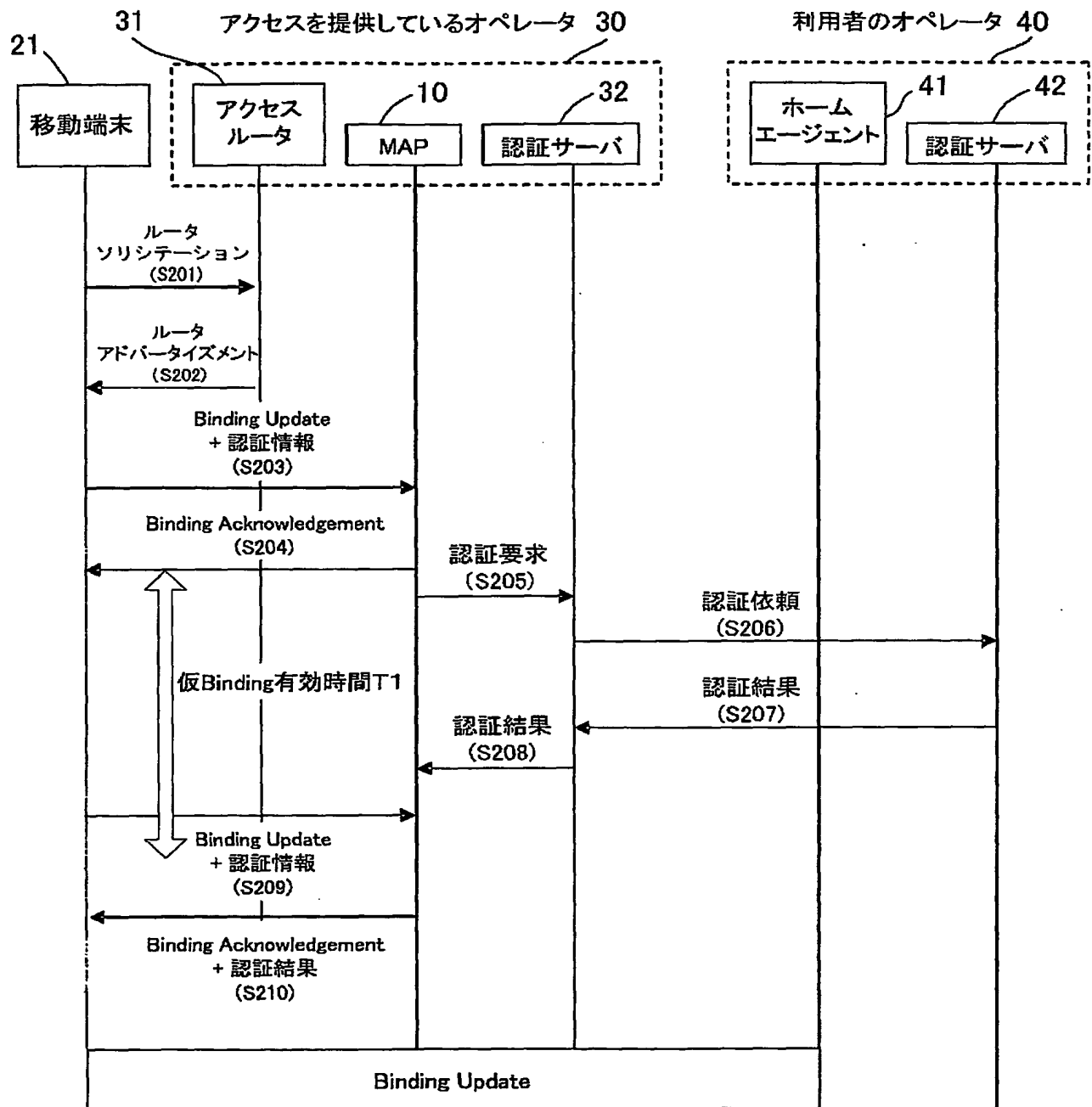


FIG. 4



5/10

FIG. 5

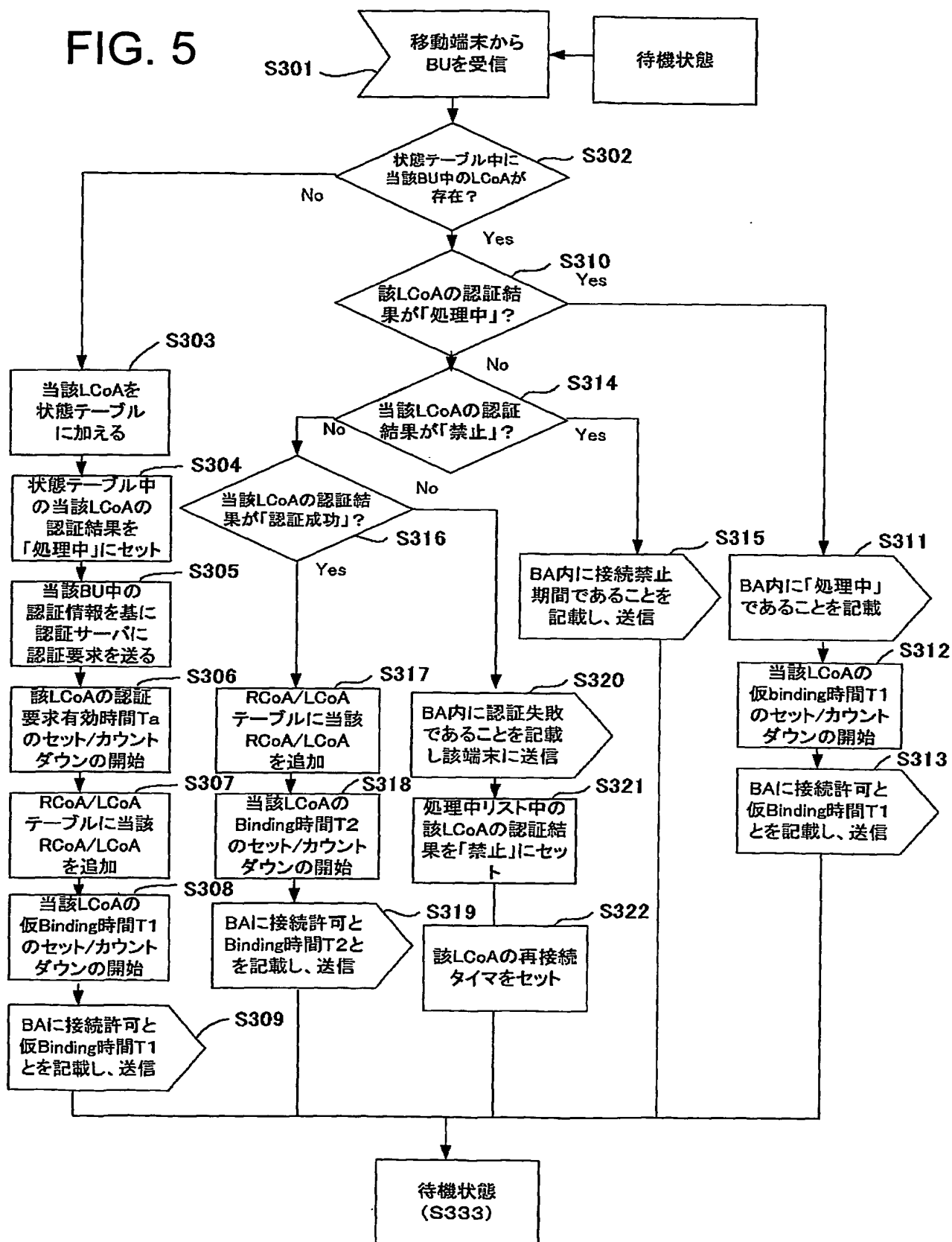


FIG. 6

端末の LCoA	認証結果	認証要求有効時間 Ta	認証要求再開時間 Tr	仮Binding時間T1 Binding時間T2
2002 :: ID101	処理中	87	—	45
2002 :: ID11	認証失敗	—	1532	—
2002 :: ID334	認証成功	—	—	231003
...

7/10

FIG. 7

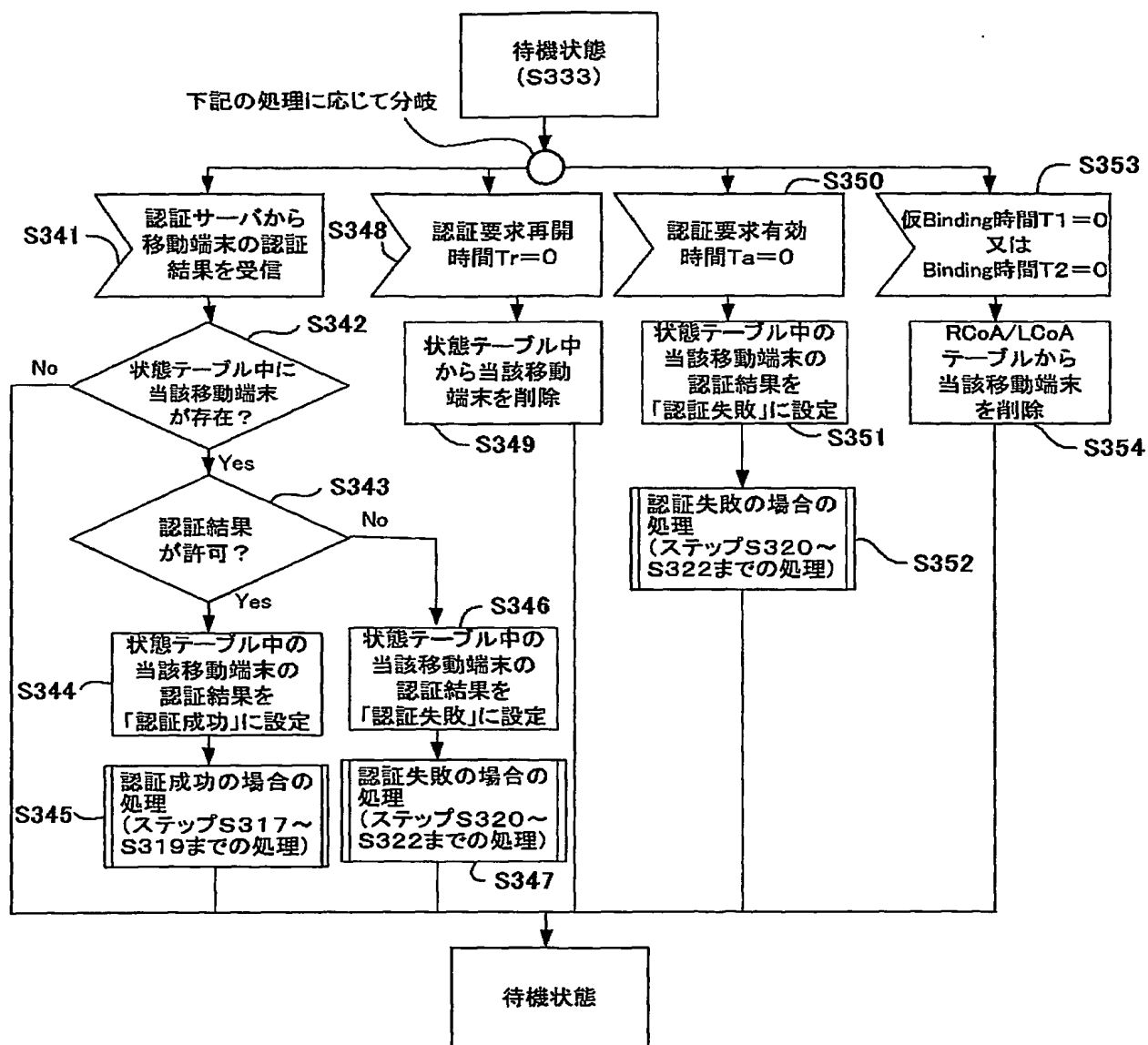


FIG. 8

端末ID	認証結果	認証要求有効時間 Ta	認証要求再開時間 Tr	仮Binding時間T1 Binding時間T2
MT101	処理中	87	—	45
MT11	認証失敗	—	1532	—
MT334	認証成功	—	—	231003
...

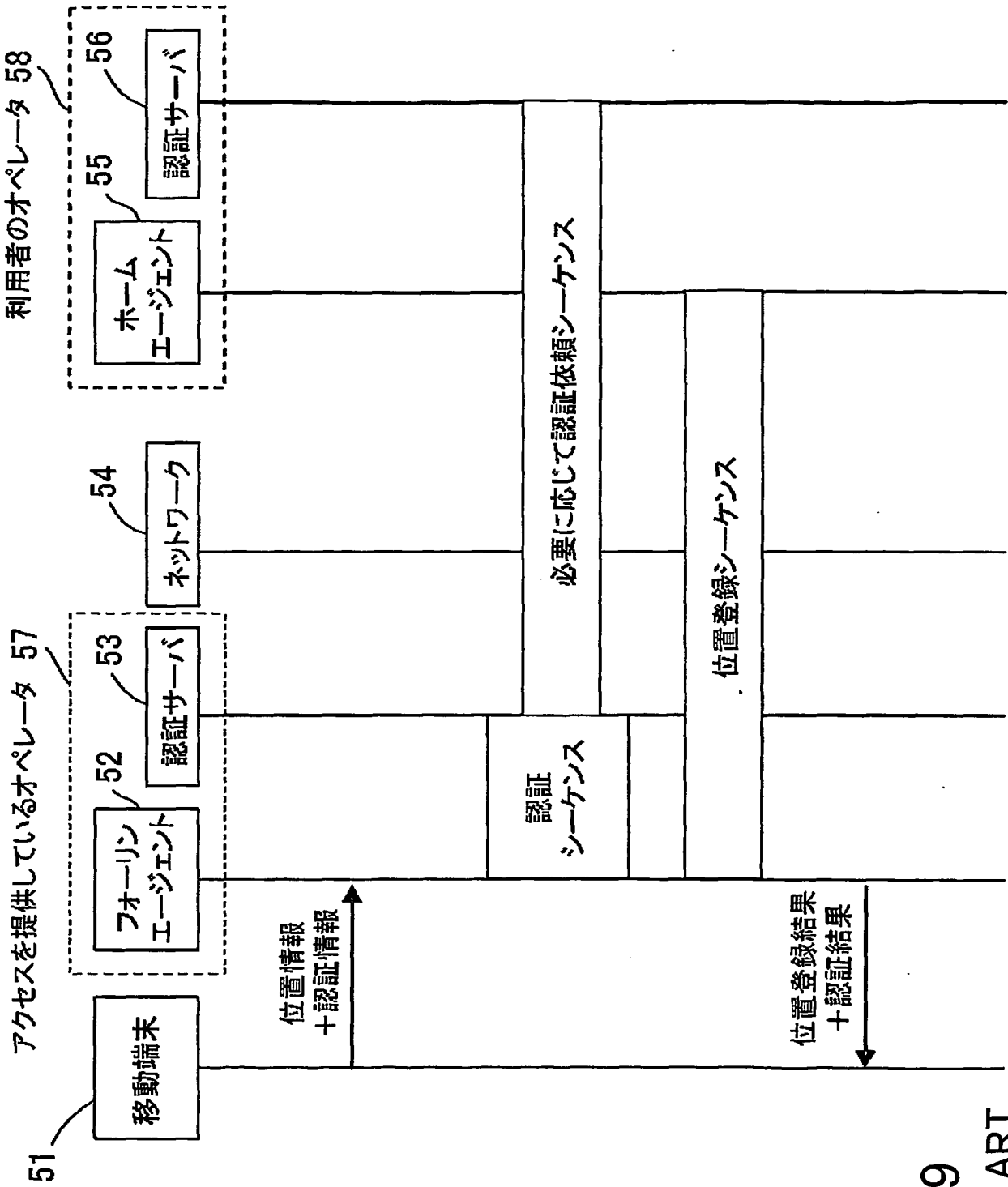


FIG. 9
PRIOR ART

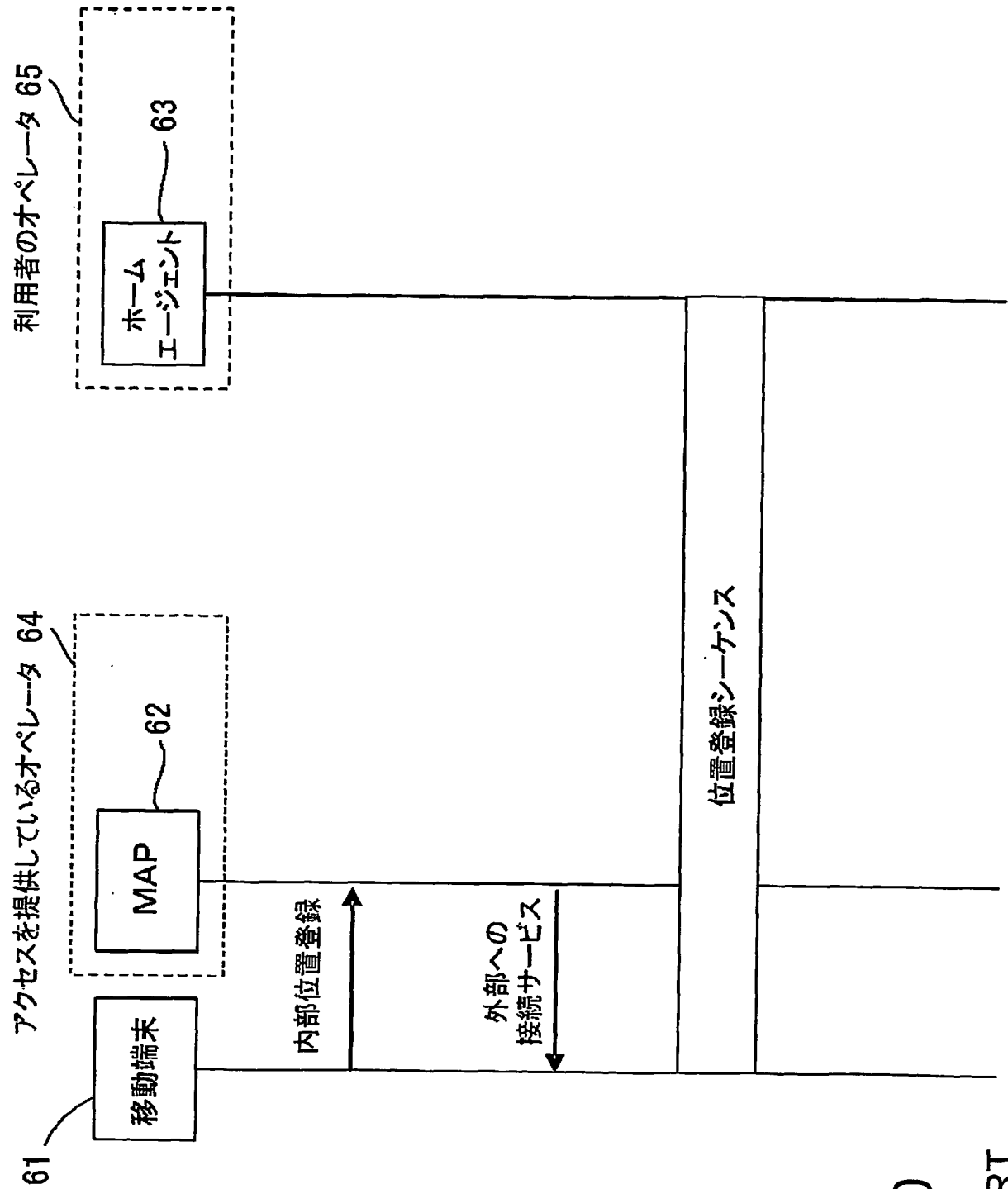


FIG. 10
PRIOR ART

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/13624

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ H04Q7/38, H04L12/56

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ H04Q7/00-7/38, H04L12/56

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2002-185520 A (Fujitsu Ltd.), 28 June, 2002 (28.06.02), Fig. 11; Par. Nos. [0035] to [0053] & US 2002/0071417 A1	1-7, 11-14, 18-26, 30-33, 37-39
Y	WO 01/067798 A (TELEFONAKTIEBOLAGET ERICSSON LM(publ)), 13 September, 2001 (13.09.01), Full text & JP 2003-526297 W & EP 1260113 A1 & AU 200136319 A & US 2001/0046223 A1	1-7, 11-14, 18-26, 30-33, 37-39 8-10, 15-17, 27-29, 34-36
A	JP 2002-271376 A (Sony Corp.), 20 September, 2002 (20.09.02), Full text & US 2002/00172207 A1	1-39

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
09 February, 2004 (09.02.04)

Date of mailing of the international search report
24 February, 2004 (24.02.04)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04Q 7/38Int. Cl⁷ H04L12/56

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04Q 7/00 - 7/38Int. Cl⁷ H04L12/56

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年

日本国公開実用新案公報 1971-2004年

日本国登録実用新案公報 1994-2004年

日本国実用新案登録公報 1996-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 2002-185520 A (富士通株式会社) 2002.06.28, 図11、第35-53段落 &US 2002/0071417 A1	1-7, 11-14, 18 -26, 30-33, 37 -39
Y	WO 01/067798 A (TELEFONAKTIEBOLAGET ERICSSON L M(publ)) 2001.09.13, 全文 &JP 2003-526297 W	1-7, 11-14, 18 -26, 30-33, 37 -39
A	&EP 1260113 A1 &AU 200136319 A &US 2001/0046223 A1	8-10, 15-17, 2 7-29, 34-36

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的な技術水準を示すもの

「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」 口頭による開示、使用、展示等に言及する文献

「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

09.02.2004

国際調査報告の発送日

24.2.2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

青木 健

印

5 J

9571

電話番号 03-3581-1101 内線 3534

C (続き) 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 2002-271376 A (ソニー株式会社) 2002.09.20, 全文 &US 2002/00172207 A1	1-39